CAICT 中国信通院

中国网络安全产业白皮书

（2019 年）

中国信息通信研究院

2019年9月

版权声明

前　言

坚实的网络安全产业实力，是网络空间繁荣稳定、保障有力的前提和基础。习近平总书记在全国网络安全和信息化工作会议上强调，要树立正确的网络安全观，积极发展网络安全产业，做到关口前移，防患于未然，对新时代我国网络安全产业发展提出更高要求。

近年来，我国网络安全产业保持高速发展态势，2018 年我国网络安全产业规模达到 510.92 亿元，较 2017 年增长 19.2%，预计 2019 年达到 631.29 亿元，从业企业近 3000 余家，产业体系日趋健全，技术创新高度活跃，综合实力显著增强，为保障国家网络空间安全奠定了坚实的产业基础。

本白皮书是我院第四次发布网络安全产业白皮书，延续了从规模结构、政府政策、企业发展、技术进展、人才培养等维度对国内外产业进展跟踪分析，同时结合热点趋势，重点对工业互联网安全、云安全、零信任安全、“人工智能+安全”、5G 安全等五个领域进行了分析预测，最后对产业发展前景进行了展望，希望为关注网络安全产业发展的企业、政府机构以及相关单位提供参考和帮助。

在本白皮书的研究过程中，得到以下单位的支持协助，在此表示感谢（以企业名称笔画为序）：三六零安全科技股份有限公司、山石网科通信技术有限公司、上海观安信息技术股份有限公司、中国电子科技网络信息安全有限公司、北京天地和兴科技有限公司、北京天融

信网络安全技术有限公司、北京字节跳动科技有限公司、北京安天网络安全技术有限公司、北京神州绿盟信息安全科技股份有限公司、北京威努特技术有限公司、北京蔷薇灵动科技有限公司、亚信科技（成都）有限公司、阿里云计算有限公司、启明星辰信息技术集团股份有限公司、杭州安恒信息技术股份有限公司、杭州迪普科技股份有限公司、奇安信科技集团股份有限公司、重庆贝特计算机系统工程有限公司、深圳市腾讯计算机系统有限公司、深信服科技股份有限公司。

目 录

一、全球网络安全产业发展情况

（一）国际网络安全政策措施持续加码

面对日益严峻的网络安全形势，美国、以色列、欧盟等国家和地区积极采取了系列政策措施，积极夯实网络安全产业基础，加速推动网络安全产业发展。

1．美国密集出台网络安全法案及政令

为落实《国家网络战略》中“加强联邦网络和关键基础设施的网络安全”的要求，美国在能源、政府等领域出台了多项网络安全法案。**在能源领域**，美国参议院于2018年12月通过《保护能源基础设施法案》；众议院于2019年1月引入了《管道和液化天然气设施网络安全预备法案》，要求管理和预算办公室加大财政投入，以提高美国能源基础设施抵御网络威胁的能力。**在政府领域**，2019年4月，美国国会引入《州网络弹性法案》，支持各州扩大网络安全产品和服务采购，并为各州解决网络安全问题提供资金支持；2019年6月，美国众议院通过了《物联网设备安全改进法案》，该法案通过提高政府物联网设备供应商的标准，利用政府的购买力来推动物联网安全市场的发展。

2．以色列积极推动网络安全国际合作

以色列高度重视依托网络安全国际合作助力网络安全产业发展，2018年以色列网络安全产业出口额超过50亿美元[1]，居于全球领先地位。**一是**积极承办高规格国际网络安全会议。以色列在2018年11月

[1] 数据来源：新华社，《以色列总理敦促加强网络安全国际合作》，2019.1.30

至 2019 年 2 月内，连续举办了国际国土安全与网络会议、国际网络安全大会、国际城市网络数据安全峰会等多个与网络安全密切相关的国际会议。**二是**强化网络安全能力输出。2019 年 4 月，以色列政府与厄瓜多尔电信和信息社会电子政务部达成合作，以色列网络安全企业将参与厄瓜多尔的网络安全建设。5 月，中国山东省举办了第 22 届“走向以色列”论坛，促进以色列网络安全企业与当地金融机构、产业集团的投资与技术合作。6 月，以色列经济和产业部与以色列国家网络局宣布同世界银行签署协议，以色列将为发展中国家提供网络安全产业支持。**三是**持续吸引网络安全领域外资投入。2018 年以色列网络安全初创企业共筹集了 10.33 亿美元的资金，资金总额同比增长 22%[2]，折射出以色列良好的网络安全产业生态对资本市场的强大吸引力。2019 年 1 月，以色列与英国建立合作伙伴关系，联合设立规模为 1.65 亿英镑的基金，用于联合投资物联网和无人驾驶汽车领域的网络安全初创企业。

3．欧洲国家加速安全能力的整合提升

欧盟近年加大了对各成员国网络安全资源的整合力度，以增强整体网络安全能力。**一是**启动网络安全能力建设计划。2019 年 3 月，欧盟宣布将投资 6350 万欧元，汇集 26 个成员国的 160 余家大型企业、创新型中小企业、高校以及网络安全研究机构，共同构建欧洲网络安全专业分析网络，加强欧盟网络安全产业协同。该计划主要包含四方

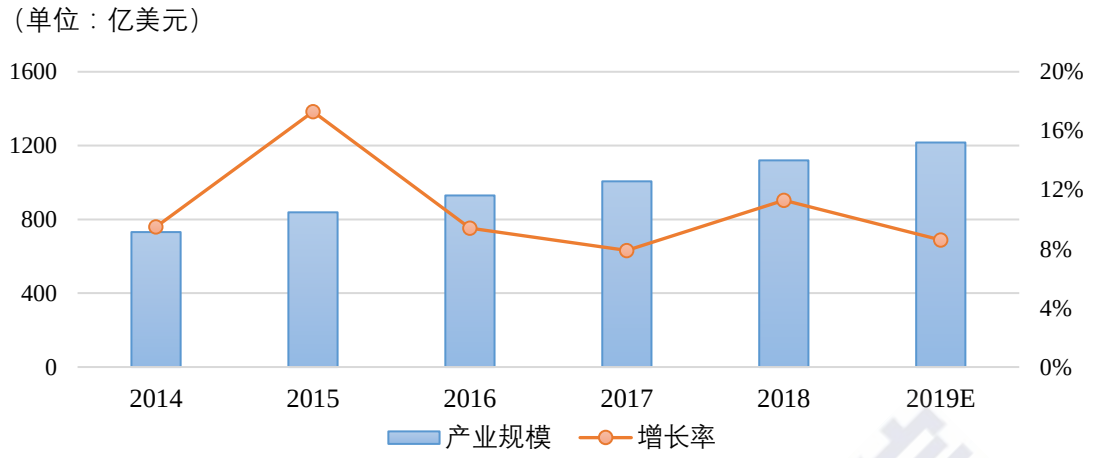
[2] 数据来源：Start-UpNation Central

面内容：整合欧盟内部网络安全资源，增强网络安全管理能力；形成政府、企业、研究机构等相关方的网络安全评估框架，进行网络预警、案例分析等；面向医疗、能源、金融、政府等行业领域，推广最佳网络安全实践；研究制定欧盟网络共同治理框架等。**二是**构建通用的网络安全认证框架。欧洲议会于 2019 年 3 月正式通过了《欧盟网络安全法案》，首次明确提出了欧盟网络安全认证计划，促进欧盟各成员国销售的认证产品、流程和服务满足统一的网络安全标准，为各成员国开发具有互操作性的网络安全产品提供便利。**三是**组织相关各方开展网络安全演习。2019 年 4 月，北约举办了代号为“锁盾”的网络安全实战演习，组织了来自法国、芬兰等 23 个国家的网络部队和大型企业的 1200 名网络安全专家参与，演习旨在强化各国在军事领域和民用领域的网络安全合作，提升网络安全事件应对和应急协同能力。

（二）全球网络安全产业规模平稳增长

2018 年全球网络安全产业规模达到 1119.88 亿美元，预计 2019 年增长至 1216.68 亿美元[3]。从增速上看，2018 年全球网络安全产业增速为 11.3%，创下自 2016 年以来的新高。2014-2019 年全球网络安全产业规模及增速如图 1 所示。

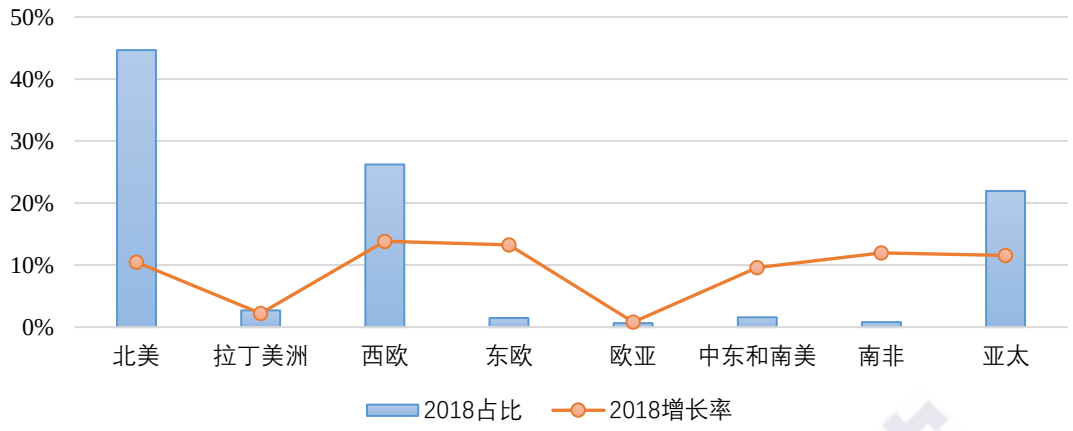
[3] 数据来源：Gartner，Information Security and Risk Management，Worldwide，2017-2023



数据来源：Gartner

图 1 2014-2019 年全球网络安全产业规模及增速

在区域分布方面，北美地区继续占据全球网络安全市场的最大份额，其次仍然为西欧和亚太地区。其中，以美国、加拿大为主的北美地区 2018 年网络安全市场规模为 500.1 亿美元，较 2017 年增长 10.45%；北美地区市场规模在全球占比为 44.66%，较 2017 年增长了 3.37 个百分点。以英国、德国、芬兰等国为主的西欧地区网络安全市场规模为 293.62 亿美元，较 2017 年增长 13.84%，增速超过亚太地区跃居全球第一；西欧地区市场规模占全球的比例为 26.22%，较 2017 年小幅上升。日本、澳大利亚等亚太地区网络安全产业规模为 245.81 亿美元，较 2017 年增长 11.54%，全球占比为 21.95%。中东、东欧、拉丁美洲等其他地区网络安全产业规模为 80.35 亿美元，全球占比为 7.18%。2018 年全球网络安全产业区域分布情况如图 2 所示。

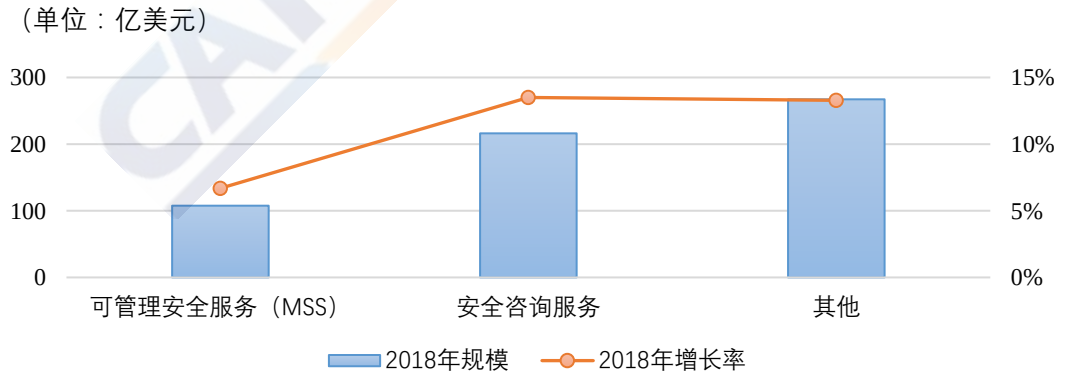


数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 2 2018 年全球网络安全产业区域分布情况

（三）网络安全细分市场格局稳中有变

根据 Gartner 统计数据，由于风险管理产品等新类别的加入，2018 年安全服务市场与安全产品市场格局由六四分趋向于五五分。其中，全球网络安全服务市场规模为 591 亿美元，较 2017 年增长 12.11%。可管理安全服务（MSS[4]）、安全咨询服务市场份额分别为：18.21%和 36.58%，如图 3 所示。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 3 2018 年全球网络安全服务市场份额及增长情况

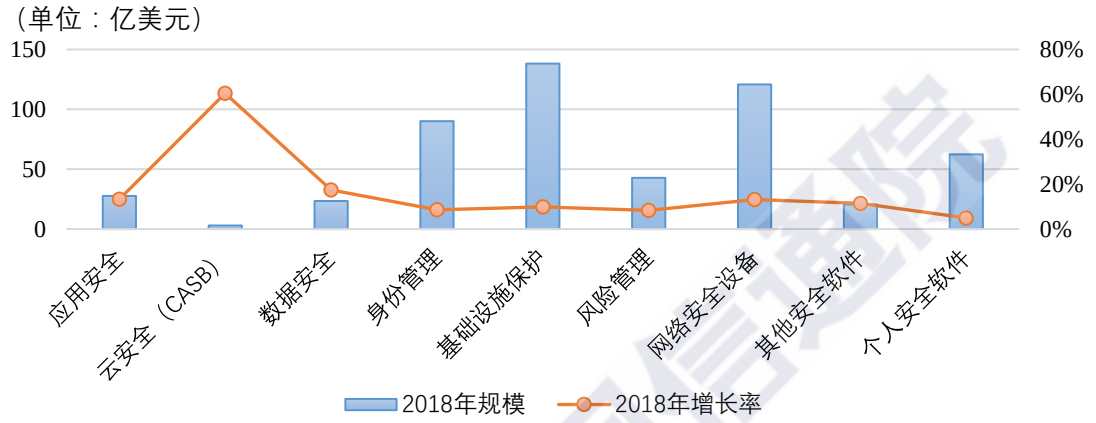
[4] MSSP：Managed Security Services，可管理安全服务

可管理安全服务市场规模达到 107.63 亿美元，相比 2017 年增长 6.69%[5]。其中，89%的市场收入来自于商品化服务，11%的市场收入来自于差异化服务。商品化服务包括安全网关/防火墙、入侵防御、设备管理、漏洞扫描等。差异化服务主要包括专业安全检测和响应、IaaS[6]及 SaaS[7]级安全监测、OT[8]和 IoT[9]安全管理和威胁情报等。2018 年，专业安全检测和响应市场规模达到近 6 亿美元，比 2017 年增长 20%。**安全咨询服务**市场规模达到 216.16 亿美元，相比 2017 年增长 13.5%[10]。德勤、安永、普华永道、毕马威、埃森哲分别以 28.56 亿、21.58 亿、20.64 亿、15.48 亿、11.25 亿占据市场前五。AT&T[11]收购 AlienVault[12]、Verizon[13]相继收购 Niddel[14]和 ProtectWise[15]，积极布局安全咨询服务市场。

2018 年全球网络安全产品市场规模达到 528.88 亿美元，较 2017 年增长 10.38%。市场份额最高的三类依次是基础设施保护、网络安全设备、身份管理。基础设施保护类产品包括企业级终端防护、安全邮件网关、Web[16]网关、安全事件管理（SIEM[17]）、威胁情报软件等，

[5] 数据来源：Gartner，Market Share Analysis: Managed Security Services, Worldwide, 2018
[6] IaaS：Infrastructure as a Service，基础设施即服务
[7] SaaS：Software as a Service，软件即服务
[8] OT：Operational Technology，运营技术
[9] IoT：Internet of Things，物联网
[10] 数据来源：Gartner，Market Share Analysis: Security Consulting Services, Worldwide, 2018
[11] AT&T：美国电话电报公司，成立于 1877 年，电信公司
[12] AlienVault：硅谷初创企业，网络安全公司
[13] Verizon：威瑞森电信，成立于 2000 年，无线通信公司
[14] Niddel：初创企业，网络安全公司
[15] ProtectWise：成立于 2013 年，软件安全初创企业
[16] Web：World Wide Web，全球广域网
[17] SIEM：security information and event management，安全事件管理

市场规模为 138.22 亿美元，占比为 26.13%。网络安全设备主要包括防火墙和入侵防御产品（IPS[18]），市场规模为 120.80 亿美元，占比为 22.84%。身份管理类产品包括访问控制、身份治理和特权账户管理，市场规模为 90.15 亿美元，占比为 17.04%，如图 4 所示。



数据来源：中国信息通信研究院（基于 Gartner 数据整理）

图 4 2018 年全球网络安全产品市场份额及增长情况

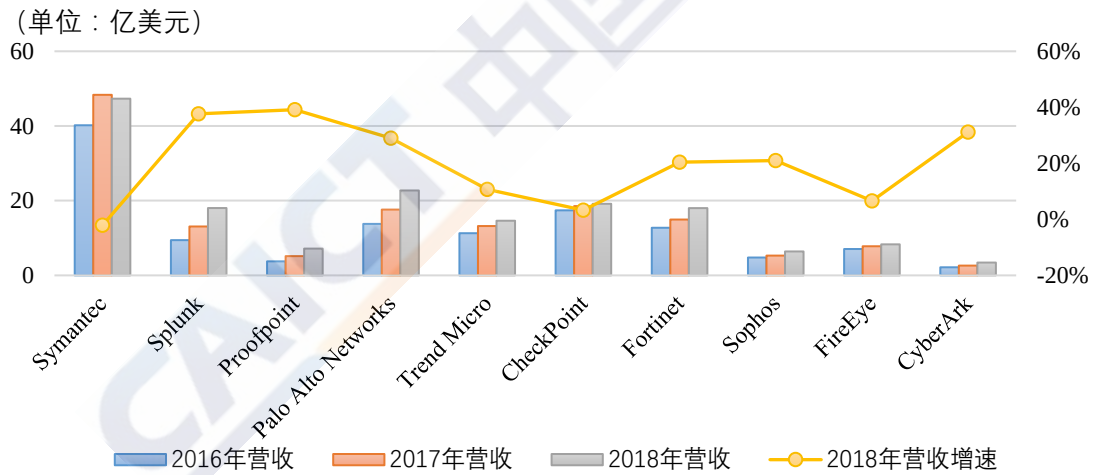
增速方面，排名前三的网络安全产品类别是云访问安全代理（CASB[19]）、数据安全以及应用安全。其中，云访问安全代理产品市场增速达到 60.47%，受益于企业上云浪潮和云安全事件的高频曝光，为更有效、更可见的实施云服务管理，云访问安全代理日益成为类似“防火墙”的标配级产品。数据安全产品市场增速达到 17.46%，欧盟 GDPR[20]等更严格的合规需求驱动企业部署加密、令牌和数据防泄漏等产品。应用安全产品市场增速达到 13.34%，驱动因素包括：移动化办公引发的终端安全需求以及应用安全测试需求的持续上升等。

[18] IPS：Intrusion Prevention System，入侵防御系统
[19] CASB：Cloud Access Security Broker，云访问安全代理
[20] GDPR：General Data Protection Regulation，通用数据保护条例

（四）上市安全企业发展态势总体良好

1．企业业绩呈现两极分化趋势

在营收方面，2018 年上市网络安全企业营收保持普长态势，营收增速差距悬殊。包括 CheckPoint[21]、Symantec[22]、Palo Alto Networks[23]、Trend Micro[24]等在内的 10 家典型网络安全企业平均营收为 16.52 亿美元，较 2017 年增长 12.67%，平均营收增幅较 2017 年度明显下降。其中，Proofpoint[25]、Splunk[26]、CyberArk[27]营收增速分别为 39.14%、37.73%、31.14%，而 Symantec、CheckPoint、Trend Micro 等老牌厂商增速低迷。2016-2018 年国际主要上市网络安全企业营收情况如图 5 所示。

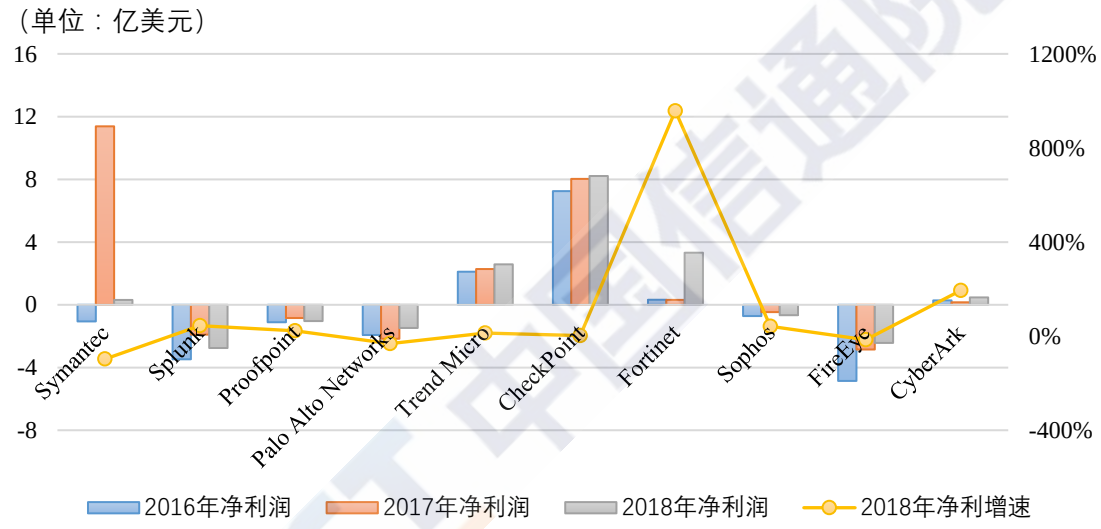


数据来源：中国信息通信研究院（基于上市企业财报整理）

图 5 2016-2018 年国际主要上市网络安全企业营收情况

[21] CheckPoint：总部位于以色列特拉维夫，网络安全解决方案供应商
[22] Symantec：赛门铁克，全球知名信息安全解决方案提供商
[23] Palo Alto Networks：派拓网络，创立于 2005 年
[24] Trend Micro：趋势科技，网络安全软件及服务提供商
[25] Proofpoint：证据点，美国著名网络安全公司
[26] Splunk：成立于 2003 年，全球知名大数据公司
[27] CyberArk：赛博埃克，安全软件公司

在净利润方面，上市网络安全企业呈现盈亏并存局面。2018 年，10 家典型网络安全企业平均净利润为 0.65 亿美元，相较于 2017 年进一步下降。研发投入的持续增长、员工分红计划实施以及激烈的市场竞争驱动的营销费用增长，增加了上市企业的运营压力，Splunk、Palo Alto Networks、Sophos[28]等企业净利润告负。2016-2018 年国际主要上市网络安全企业净利润情况如图 6 所示。



数据来源：中国信息通信研究院（基于上市企业财报整理）

图 6 2016-2018 年国际主要上市网络安全企业净利润情况

在研发投入方面，2018 年上市网络安全企业研发投入普涨，研发投入占营收比例保持高位。10 家典型网络安全企业的平均研发投入增长为 18.28%。其中 Symantec 研发投入略有降低，但仍保持在 9 亿美元高位，远超其他厂商；Splunk 研发投入增加了 46.89%至 4.38 亿美元，位列第二；Palo Alto Networks 研发投入增长了 15.34%至 4.01

[28] Sophos：守护使，IT 安全与保护公司

亿美元，位列第三；其余企业未超过 2 亿美元。2018 年 10 家典型网络安全企业的平均研发投入占营收比例为 20.15%，持续的高研发投入占比为企业抢占技术先机、保持可持续发展奠定重要基础。2016-2018 年国际主要上市网络安全企业研发投入情况如图 7 所示。

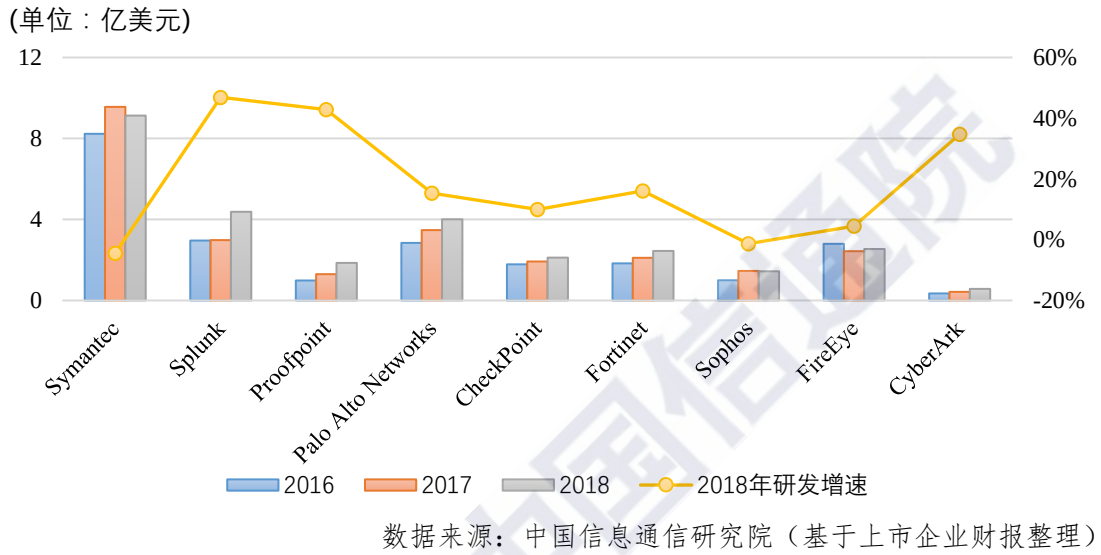


图 7 2016-2018 年国际主要上市网络安全企业研发投入情况[29]

2. 安全企业上市步伐保持稳定

据不完全统计，2018 年 6 月至 2019 年 5 月，国际上已有 4 家网络安全企业实现上市融资。此外，Crowdstrike[30]、Palantir[31]和 Ping Identity[32]也计划于 2019 年上市。2018 年 6 月至 2019 年 5 月国际网络安全企业 IPO 情况如表 1 所示。

[29] 说明：Trend Micro 未披露研发费用
[30] Crowdstrike：成立于 2011 年，网络安全公司
[31] Palantir：成立于 2004 年，总部位于美国帕罗奥多
[32] Ping Identity：成立于 2002 年，身份管理服务公司

表 1 2018 年 6 月至 2019 年 5 月国际网络安全企业 IPO 情况

上市时间	企业名称	技术领域	募集资金（亿美元）
2019.04	Tufin	安全策略管理	1.08
2018.10	SolarWinds	IT 基础设施管理	3.75
2018.07	Tenable	漏洞管理	2.51
2018.06	Avast	防病毒	7.65

数据来源：中国信息通信研究院根据公开资料整理

Tufin 创立于 2005 年，总部位于以色列拉马特甘，创始人兼 CEO Ruvi Kitov 和 CTO Reuven Harrison 曾在 Check Point 任职。Tufin 致力于安全策略的可视化运营管理，可基于局域网、私有云、公共云、混合云等不同环境提供高效地网络安全规划和管理。2018 年，Tufin 营业收入达 8500 万美元，较 2017 年增长 31.7%。目前 Tufin 在在全球拥有 2000 多家客户，覆盖近半数的财富 50 强企业。

SolarWinds 创立于 1999 年，总部位于美国得克萨斯州奥斯汀，曾于 2009 年上市，后于 2015 年私有化退市，2018 年再次上市。SolarWinds 聚焦于网络性能管理、网络监控和恢复等领域，曾收购邮件安全、日志管理、数据库管理、网络流量监控等技术方向的 10 余家企业。2018 年，SolarWinds 营业收入达 8.83 亿美元，较 2017 年增长 14.43%。

Tenable 由 Renaud Deraison、Ron Gula 及 Jack Huffard 创立于 2002 年，总部位于美国哥伦比亚。Tenable 曾于 2012 年获得来自 In-Q-tel 的 5000 万美元 A 轮融资，并于 2015 年获得来自 Insight Venture

Partners[33]和 Accel[34] 的 2.5 亿美元 B 轮投资。Tenable 作为漏洞扫描软件 Nessus 的开发者，开创了漏洞管理市场，其产品网络曝光平台（Cyber Exposure）可实现跨攻击面的网络风险评估和漏洞管理。2018 年，Tenable 营业收入达 2.67 亿美元，较 2017 年增长 42.4%，全球用户超过 27000 家。

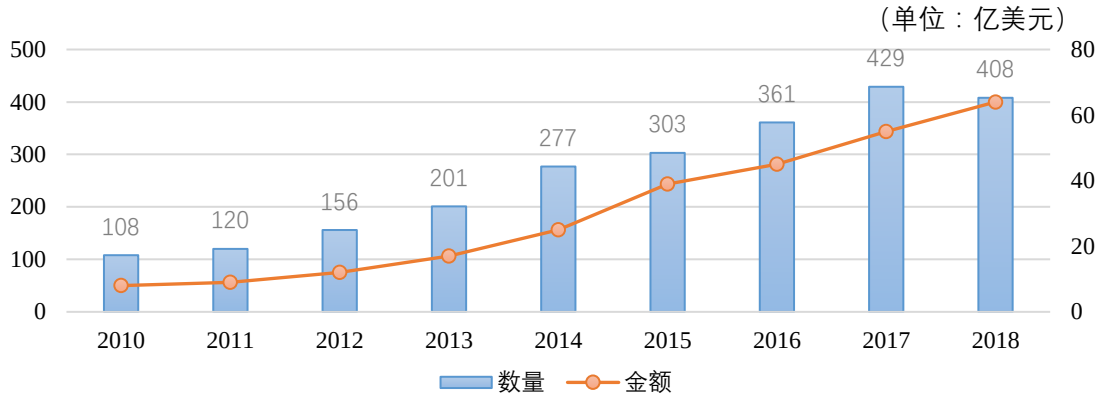
Avast 由 Pavel Baudiš and Eduard Kučera 创立于 1988 年，总部位于捷克首都布拉格。Avast 以杀毒软件起家，目前主营业务包括防病毒产品、安全网关、安全托管平台及服务等。Avast 于 2016 年以 13 亿美元收购了同样成立于捷克的 AVG Technologies[35]，2018 年在伦敦证券交易所上市。2018 年，Avast 营业收入达 8.08 亿美元，较 2017 年增长 24%，其产品的全球活跃用户数超过 4.35 亿。

（五）网络安全融资并购活动持续活跃

1．融资数量小幅回落，交易总额持续增长

2018 年，国际网络安全产业的融资活动数量达到 408 起，较 2017 年下降 4.95%，近年来首次回落，但仍处于高位水平；交易总额为 64 亿美元，增长了 16.36%，如图 8 所示。

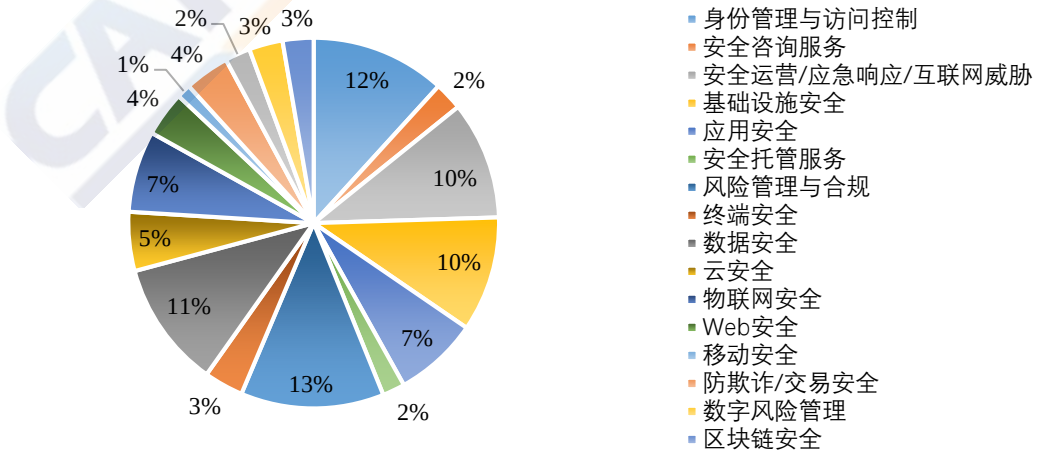
[33] Insight Venture Partners：总部位于美国纽约，风险投资公司
[34] Accel：总部位于美国加州，风险投资公司
[35] AVG Technologies：总部位于荷兰，安全软件厂商



数据来源：Momentum Cyber

图 8 2010-2018 年网络安全初创企业融资态势

从融资的技术领域来看，风险管理与合规、身份管理与访问控制、数据安全等领域融合活动占比均超过 10%，融资数量分别达到 53 起、49 起、45 起。从融资轮次分布看，2018 年共有 142 家的企业位于天使轮阶段，交易总额为 5 亿美元；处于 A 轮的企业有 85 家，交易总额为 7 亿美元；有 60 家企业处于 B 轮阶段，交易总额为 14 亿美元；位于 C+轮的有 103 家，交易总额为 35 亿美元。2018 年全球网络安全融资领域分布情况如图 9 所示。

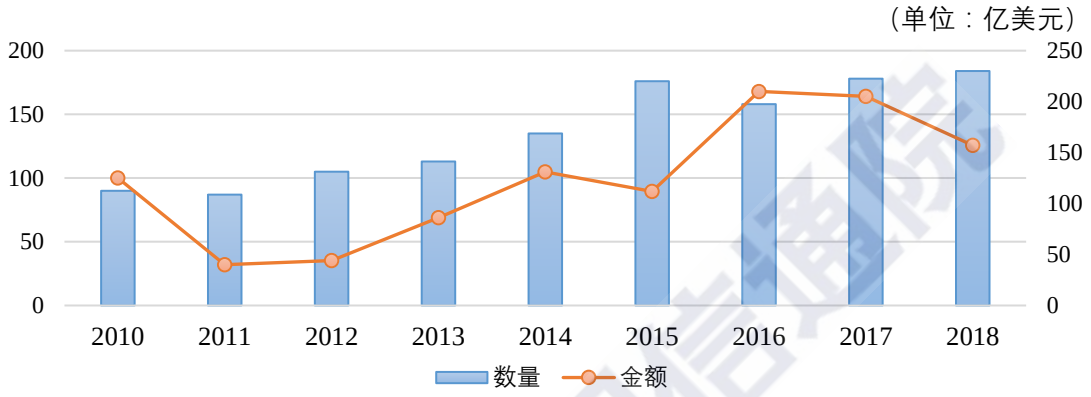


数据来源：Momentum Cyber

图 9 2018 年全球网络安全融资领域分布情况

2．并购数量再创新高，热点领域发生变化

据不完全统计，2018 年国际网络安全产业的并购活动数量再创新高，达到 184 起，较 2017 年增长了 6 起；交易总额为 157 亿美元，较 2017 年有所回落，如图 10 所示。



数据来源：Momentum Cyber

图 10 2010-2018 年全球网络安全并购活动态势

从并购交易方看，**一是**私募公司依然在网络安全领域并购活动中扮演重要角色，例如 Thoma Bravo[36]以 16 亿美元收购数据安全厂商 Barracuda Networks[37]后，又相继以 21 亿美元、5.25 亿美元、9.5 亿美元收购 Imperva[38]、LogRhythm[39]、Veracode[40]三家安全企业；**二是**大型 IT 企业并购交易活动部分涉及网络安全，例如 IBM[41]以 340 亿美元收购 Redhat[42]、Broadcom[43]以 189 亿美元收购 CA Technologies[44]、General

[36] Thoma Bravo：总部位于美国，私募股权投资公司
[37] Barracuda Networks：梭子鱼网络，成立于 2002 年，总部位于美国硅谷
[38] Imperva：总部位于美国，数据应用安全服务商
[39] LogRhythm：成立于 2003 年，总部位于美国科罗拉多州博尔德市
[40] Veracode：成立于 2006 年，应用程序安全公司
[41] IBM：International Business Machines Corporation，国际商业机器公司
[42] Redhat：红帽公司，开源解决方案供应商，总部位于美国北卡罗来纳州的罗利市
[43] Broadcom：博通公司，有线和无线通信、半导体公司
[44] CA Technologies：成立于 1976 年，总部位于美国纽约长岛

Dynamics[45]以 68 亿美元收购 CSRA Inc[46]等，三家被收购的 IT 综合服务企业均有网络安全业务；**三是**安全企业积极通过并购实现能力拓展，例如 Cisco[47]收购 Duo Security[48]布局零信任安全，Splunk 收购 Phantom Cyber[49]增强安全编排自动化与响应能力，Palo Alto Networks 收购 Evident.io[50]提升云服务基础设施安全能力。2018 年值得关注的典型网络安全并购活动如表 2 所示。

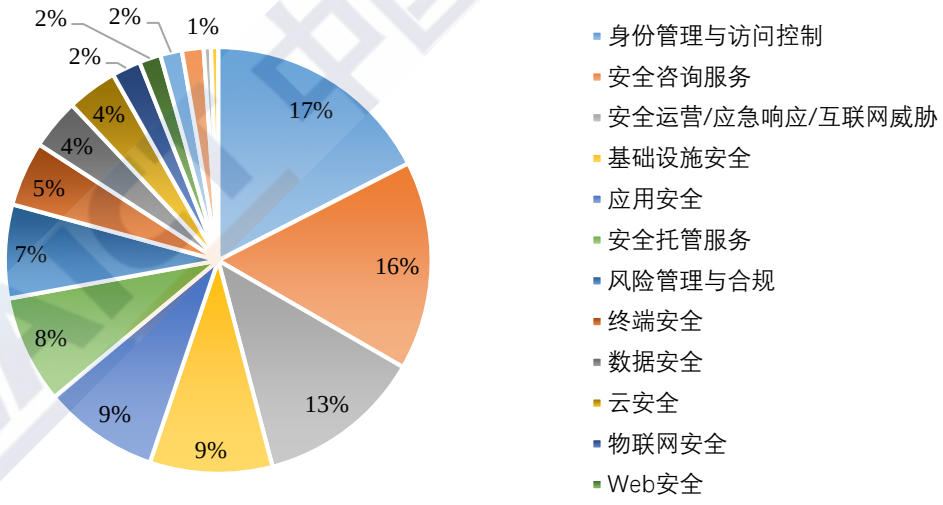
表 2 2018 年值得关注的网络安全并购活动[51]

日期	被收购方	并购方	技术领域	金额（亿美元）
2018.1	ThreatMetrix	Relx Group	身份认证	8.17
2018.2	PhishMe	BlackRock and Pamplona Capital	防钓鱼攻击	4
2018.2	Phantom Cyber	Splunk	安全编排自动化响应（SOAR[52]）	3.5
2018.6	SimpliSafe	Hellman & Friedman	智能家居安全	10
2018.7	Syntel	Atos	大数据安全	35.7
2018.8	Duo Security	Cisco	零信任	23.5
2018.8	InfoArmor	Allstate	威胁情报	5.25
2018.10	Imperva	Thoma Bravo	应用安全	21
2018.11	Cylance	Blackberry	基于 AI[53]的网络安全	14
2018.11	Veracode	Thoma Bravo	应用安全	9.5

来源：中国信息通信研究院根据公开资料整理

[45] General Dynamics：通用动力，美国国防企业集团
[46] CSRA Inc：总部位于美国弗吉尼亚州费尔法克斯，信息技术&IT 技术企业
[47] Cisco：思科，网络解决方案供应商
[48] Duo Security：总部位于美国密歇根州，企业级移动认证安全公司
[49] Phantom Cyber：总部位于美国加州，安全自动化公司
[50] Evident.io：成立于 2013 年，公共云安全服务公司
[51] 说明：表格中日期为交易意向披露或成交完成日期
[52] SOAR：Security Orchestration and Automation Response，安全编排自动化与响应
[53] AI： Artificial Intelligence，人工智能

从并购的细分领域看，身份管理与访问控制、安全咨询与安全运营成为了 2018 年最热门的选择。其中，身份管理与访问控制领域共有 32 起并购活动，比 2017 年的 25 起增加了 28%。伴随云计算、物联网、5G[54]等新一代信息技术的发展，设备、平台、应用数量指数级增长，网络生态融合化、开放化发展，大幅增加了网络安全管理的复杂度，驱动身份管理与访问控制市场需求不断上升，激发了并购热潮。安全咨询、安全运营领域分别有 29 起、24 起并购活动，一方面是受益于 GDPR 等合规需求，另一方面勒索病毒、数据泄露等安全事件增加了对安全规划设计、运营服务、应急响应等方面的安全需求。2018 年全球网络安全并购领域分布情况如图 11 所示。



数据来源：Momentum Cyber[55]

图 11 2018 年全球网络安全并购领域分布情况

[54] 5G：Fifth-Generation Mobile Networks，第五代移动通信
[55] Momentum Cyber：网络安全咨询公司

（六）网络安全人才短缺情况尚未缓解

1．网络安全人才短缺问题日趋严峻

根据 2018 年(ISC)2 网络安全劳动力研究报告，全球网络安全人才缺口已扩大至近 300 万。其中，亚太地区缺口最高，达到了 214 万，北美地区以近 50 万的人才缺口排名第二。针对企业网络安全人员配置，63%的受访人员认为企业存在网络安全人员短缺的情况，59%受访人员认为他们的公司正因人才短缺面临中度或高度风险，48%的受访人员认为他们的组织计划在未来一年内增加网络安全人员配置。

2．各国积极探索网络安全人才培养新举措

美国通过多渠道不断完善其网络安全人才培养体系。**一是**发布全新网络安全人才计划。美国总统特朗普于 2019 年 5 月签署关于美国网络安全人才队伍的行政令，提出设立联邦政府网络安全人才轮岗机制、开展“总统杯”网络安全竞赛、向优秀网络安全人才颁发“总统级”嘉奖等。**二是**促进公私部门的网络安全人才交流。2019 年 3 月，美国参议院提出《网络安全交流法案》，拟建立一个公私部门网络安全从业人员的交流计划，通过整合联邦政府、私营部门和学术机构的网络安全人才资源，以弥补美国在国防和关键基础设施领域的网络安全技术人才缺口。**三是**加大网络安全人才培养支持力度。美国国家科学基金会（NSF[56]）将四所高校新纳入“CyberCorps：服务奖学金”（SFS）计划，四所高校将在 2018-2019 年获得近 570 万美元用于网络安全科

[56] NSF：National Science Foundation，美国国家科学基金会

研和人才培养。

英国积极打造网络教育中心。2018 年，英国国家网络安全中心（NCSC[57]）在格洛斯特郡新建了两个网络教育试点中心，将网络安全技能培养作为重要方向，提供各类教育资源。

新加坡实施网络安全领域孵化计划。2018 年 3 月，新加坡政府推出创新网络安全生态（Innovation Cybersecurity Ecosystem）孵化计划，由新加坡网络安全局资讯和通信媒体发展局联合资助，计划在两年内面向 100 名网络安全创业者提供培训，孵化 40 家初创企业。

二、我国网络安全产业发展进展

（一）产业发展政策环境持续优化

1．国家网络安全领域法律法规加紧制定

一是网络安全相关立法计划稳步推进。《电信法》《数据安全法》列入十三届全国人大常委会立法规划，相关研制论证工作有序开展。2019 年 7 月，由国家密码管理局起草的《中华人民共和国密码法（草案）》在全国人大网公布，向社会公开征求意见。由中央网信办、工业和信息化部、公安部负责起草的《关键信息基础设施安全保护条例》列入国务院 2019 立法计划，有望年内正式出台。《网络安全等级保护条例》已于 2018 年 6 月向社会公开征求意见。**二是网络安全领域重要制度建设明显加快。**2019 年 5 月以来，《网络安全审查办法》《数据安全管理办法》《儿童个人信息网络保护规定》《网络关键设备安全检

[57] NCSC：National Cyber Security Centre(United Kingdom)，英国国家网络安全中心

测实施办法》《个人信息出境安全评估办法》《网络安全漏洞管理规定》等重要制度相继完成向社会公开征求意见，进入修改完善阶段。2019年7月，国家网信办、国家发展改革委、工业和信息化部、财政部联合发布《云计算服务安全评估办法》，对党政机关、关键信息基础设施运营者采购使用的云计算服务提出更高安全要求。

2．重要行业和新兴领域安全要求细化明确

一是电力、工业互联网、车联网等重要行业领域网络安全顶层设计密集出台。2018年9月，国家能源局发布《关于加强电力行业网络安全工作的指导意见》，提出加强全方位网络安全管理、强化关键信息基础设施安全保护、提高网络安全态势感知、预警及应急处置能力等16条意见，明确了电力行业今后一段时间内网络安全工作重点。2018年12月，工业和信息化部印发《车联网（智能网联汽车）产业发展行动计划》，将“强化管理、保障安全”作为基本要求，提出了“产业安全管理体系初步形成，安全管理制度与安全防护机制落地实施，安全技术及产品研发取得阶段性成果，安全技术支撑手段建设初见成效，安全保障和服务能力逐步完善”的阶段性发展目标。2019年9月，工业和信息化部会同九部门联合印发《加强工业互联网安全工作的指导意见》，要求“加快构建工业互联网安全保障体系，形成覆盖工业互联网全生命周期的事前防范、事中监测和事后应急能力”。

二是金融科技、区块链、IPv6[58]等新兴技术领域安全发展目标和要求

[58] IPv6：Internet Protocol Version 6，互联网协议第6版

更为明确。2019 年 1 月，国家互联网信息办公室发布《区块链信息服务管理规定》，明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，规避区块链信息服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。2019 年 4 月，工业和信息化部印发《关于开展 2019 年 IPv6 网络就绪专项行动的通知》，提出“完善网络安全管理制度体系，同步升级防火墙/WAF[59]、IDS[60]/IPS[61]、4A[62]系统等 IPv6 网络安全防护手段”等系列增加网络安全保障的措施。2019 年 8 月，中国人民银行印发《金融科技（FinTech）发展规划（2019-2021 年）》，围绕大数据、云计算、人工智能等新兴技术在金融领域安全应用以及金融网络安全风险管控等提出细化措施。

3．区域性网络安全产业发展政策集中释放

一是产业专项规划明确发展重点及方向，推动产业链布局。2018 年 9 月，成都市信息化工作领导小组办公室印发《成都市网络信息安全产业发展规划（2018—2022 年）》，提出到 2022 年，将成都打造为西部领先、国内一流的网络信息安全产业高地，明确了产业发展的九个重点技术方向和六项重大工程，提出了系列保障措施。2018 年 11 月，长沙市政府发布《长沙市加快网络安全产业发展三年（2019—2021 年）行动计划》《长沙市加快网络安全产业发展的若干政策》，积极打

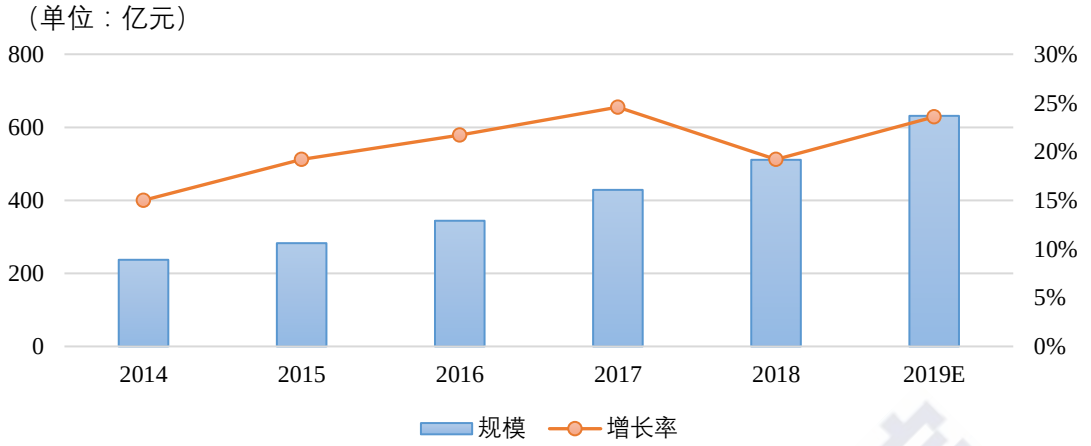
[59] WAF：Web Application Firewall，Web 应用防火墙，网站应用级入侵防御系统
[60] IDS：Intrusion Detection Systems，入侵检测系统
[61] IPS：Intrusion Prevention System，入侵防御系统
[62] 4A：Authentication, Authorization,Accounting and Audit，统一安全管理平台解决方案

造具有长沙特色的网络安全产业体系。2019 年 6 月，《国家网络安全产业发展规划》正式发布，规划提出到 2020 年，依托产业园带动北京市网络安全产业规模超过 1000 亿元，拉动 GDP 增长超过 3300 亿元，打造不少于 3 家年收入超过 100 亿元的骨干企业。工业和信息化部、北京市政府将在培育骨干企业、资金支持、人才引进和配套支撑等方面向国家网络安全产业园区提供切实有效的政策支持。**二是相关领域政策助推网络安全能力建设和产业发展。**2018 年 5 月以来，天津陆续出台《天津市关于加快推进智能科技产业发展若干政策》《促进大数据发展应用条例》，鼓励数据保护关键技术和数据安全监管支撑技术的创新和研究，支持科研机构、高等院校和企业在数据安全环节进行技术攻关，并对符合条件的项目给予资金支持。2018 年 4 月，上海印发《上海市工业控制系统信息安全行动计划（2018-2020 年）》，提出通过财税支持、标准建设、人才培养和交流合作等保障措施，提升工业控制系统信息安全的综合管理能力、安全防护能力、技术支持能力和产业发展能力。

（二）我国产业规模持续高速增长态势

1．产业规模保持高速增长

根据中国信息通信研究院统计测算，2018 年我国网络安全产业规模达到 510.92 亿元，较 2017 年增长 19.2%，预计 2019 年达到 631.29 亿元，如图 12 所示。



数据来源：中国信息通信研究院

图 12 2018 年我国网络安全产业规模增长情况

2. 从业企业数量小幅增长

据不完全统计，2018 年我国共有 2898 家从事网络安全业务的企业，新增企业数量为 217 家，增长率为 8.09%，保持健康发展态势。从区域分布看，北京、广东、上海依然位列前三，分别为 975 家、366 家和 288 家。

表 3 我国网络安全企业按区域分布排名前十的名单

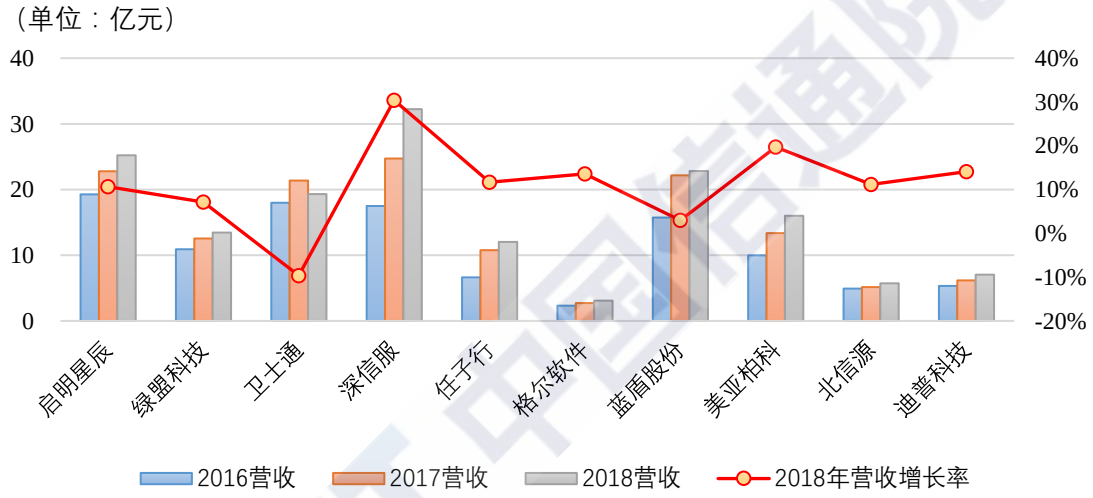
区域	企业数量	占比
北京	975	33.64%
广东	366	12.63%
上海	288	9.94%
江苏	167	5.76%
四川	139	4.80%
山东	137	4.73%
浙江	120	4.14%
福建	104	3.59%
湖北	82	2.83%
辽宁	70	2.42%

数据来源：中国信息通信研究院网络安全产业开放平台

（三）网络安全企业发展总体良好

1．上市企业业绩保持平稳增长

在营收规模方面，企业营收规模总体呈稳定增长态势。10 家上市网络安全企业 2018 年平均营收规模为 15.69 亿元，较 2017 年的 14.18 亿元增长了 10.69%。其中，深信服营收规模首次突破了 30 亿元，启明星辰和蓝盾股份的营收规模超过 20 亿元。2016-2018 年我国上市网络安全企业营收情况如图 13 所示。

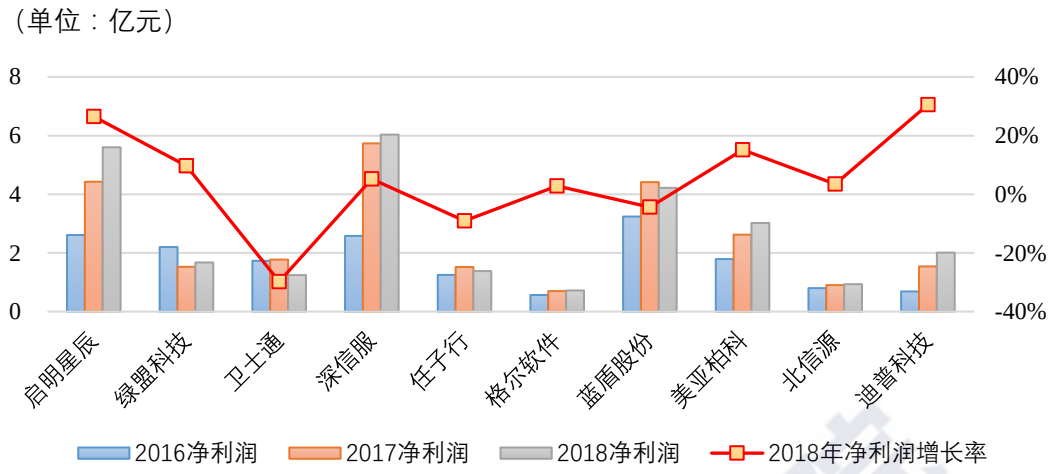


数据来源：中国信息通信研究院（基于上市企业财报整理）

图 13 2016-2018 年我国上市网络安全企业营收情况[63]

在净利润方面，企业净利润增速总体放缓，但仍远高于国际水平。10 家上市网络安全企业 2018 年平均净利润为 2.68 亿元，较 2017 年略微增长 6.67%。2016-2018 年我国上市网络安全企业净利润情况如图 14 所示。

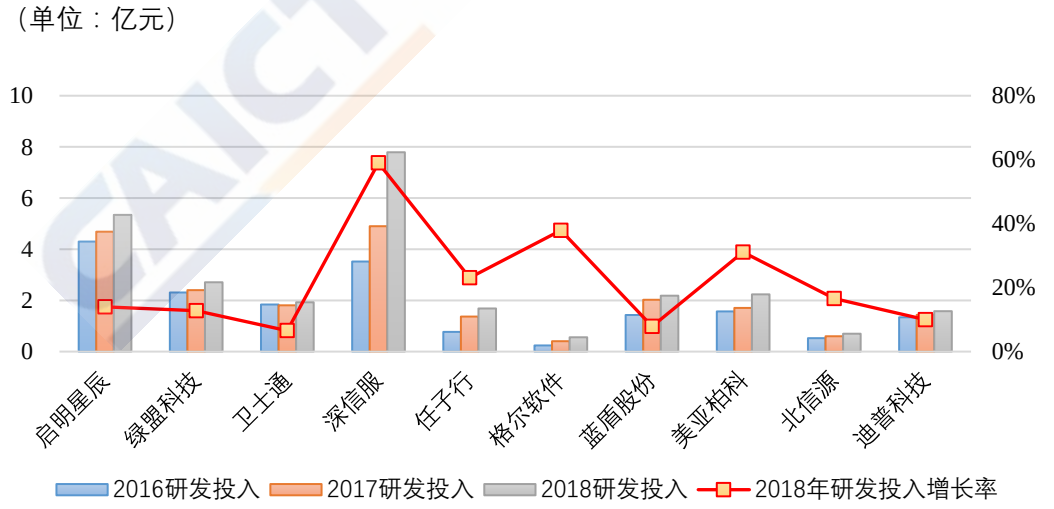
[63] 说明：部分上市企业网络安全业务占比较低，故未纳入作为典型企业分析



数据来源：中国信息通信研究院（基于上市企业财报整理）

图 14 2016-2018 年我国上市网络安全企业净利润情况[64]

在研发投入方面，企业持续加大研发投入力度。2018 年国内 10 家上市网络安全企业平均研发投入为 2.67 亿元，相较于 2017 年增长了 25.2%。2016-2018 年我国上市网络安全企业研发投入情况如图 15 所示。



数据来源：中国信息通信研究院（基于上市企业财报整理）

图 15 2016-2018 年我国上市网络安全企业研发投入情况

[64] 说明：部分上市企业网络安全业务占比较低，故未纳入作为典型企业分析

2．科创板成为企业上市快车道

目前科创板已上市和拟上市的网络安全相关企业共计6家，分别为白山云科技、安恒信息、山石网科、安博通、光通天下、连山科技，如表4所示。

表 4 我国科创板上市和拟上市网络安全企业

企业	主要领域	创立时间
安博通	IPv6安全、IoT安全、云安全、智能安全和安全可视化	2011
山石网科	云计算安全、边界安全、内网安全、数据安全、智能分析管理以及安全服务	2011
安恒信息	云安全、大数据安全、物联网安全、安全管理平台	2007
白山云科技	云分发、云安全、数据应用与集成	2015
光通天下	云计算安全、网络安全、边界安全、存储安全、应用安全	2014
连山科技	通信安全、数据安全、物联网安全、安全服务	2006

数据来源：中国信息通信研究院根据公开信息整理

安博通已于9月6日在科创板上市，成为首个登陆科创板的网络安全企业。其核心业务包括网络安全产品、安全服务等，网络安全产品主要涉及安全网关和安全管理两大类，安全服务则主要为安全产品技术开发与安全运维服务，同时安博通在IPv6安全、IoT安全、云安全、智能安全和安全可视化等领域都进行了布局。安博通本次募集资金 2.98 亿元，拟投向深度网络安全嵌入系统升级与虚拟资源池化项目、安全可视化与态势感知平台研发及产业化项目以及安全应用研发中心与攻防实验室建设项目。

山石网科于 9 月 4 日在科创板 IPO 注册生效。山石网科主要提供下一代防火墙、入侵检测和防御系统、微隔离与可视化、虚拟化防火墙、Web 应用防火墙等产品及安全服务，业务覆盖美洲、欧洲、东南亚、中东等 50 多个国家和地区，并在苏州、北京和美国硅谷设有研发中心。本次募集资金 8.94 亿元，拟投向网络安全产品线拓展升级项目、高性能云计算安全产品研发项目和营销网络及服务体系建设项目。

3．大型国企深度布局安全市场

一是中国电子信息产业集团（CEC[65]）战略入股奇安信。2019 年 5 月，CEC 与奇安信签署战略合作协议，以人民币 37.31 亿元持有奇安信 22.59%股份，成为奇安信第二大股东。双方将在技术创新、资源整合、重大项目建设等方面开展合作，推进央企网络安全响应中心、现代数字城市网络安全响应中心和“一带一路”网络安全响应中心建设。**二是**中国电子科技集团公司（CETC[66]）实施股份增持，成为绿盟科技第一大股东。2019 年 8 月，CETC 全资子公司电科投资通过集中竞价交易方式买入绿盟科技 1.6292%股份，电科投资及其一致行动人中电基金、网安基金合计持有绿盟科技 15.4990%股份，成为第一大股东。此次增持绿盟科技，将进一步完善其在网络安全领域的布局，增进旗下企业间的业务协同和优势互补，打造网络安全产业生态链。

[65] CEC：China Electronics Corporation，中国电子信息产业集团
[66] CETC：China Electronics Technology Group Corporation，中国电子科技集团有限公司

（四）产业生态环境不断优化完善

1．多地网络安全产业园区加快建设

北京国家网络安全产业园进入实质性建设阶段。2019 年 1 月，北京国家网络安全产业园挂牌。园区总占地面积 7330 亩，建筑面积 440 万平方米，拟打造成国内领先、世界一流的网络安全高端、高新、高价值产业集聚中心。截至目前，已有超过 30 余网络安全企业入驻园区或确定意向。

天津滨海信息安全产业园一期工程即将竣工。该产业园总投资 45 亿元，规划总建筑面积约 36 万平方米，其中一期工程为 8000 平方米。目前，产业园已汇集了中国反恶意软件联盟、中国可信计算联盟、国际云安全联盟、数字中国联合会信息安全产业联盟“四个联盟”，国家计算机病毒应急处理中心、计算机病毒防治技术国家工程研究中心、公安部计算机病毒防治产品检验中心三个国家级中心以及天津海洋数据中心、等级保护工程中心、互联网监控中心三个省部级中心；已有 13 家网络安全企业确认入园意向，部分已先期注册或办理搬迁手续。

湖北武汉国家网络安全人才与创新基地取得阶段性建设进展。2018 年 9 月，国家网安基地已签约落户项目 41 个，注册企业 75 家，协议投资 3262 亿元，在建项目总投资达 2000 亿元。2019 年 3 月，投资 50 亿元的国家网络安全大会永久会址、投资 20 亿元的网安文化融合创新综合体正式签约落户。

山东泰安以国际合作为核心，打造网络安全人才高地。中以-网络安全泰山产业园于2018年12月揭牌，产业园将加深中以在网络安全领域的合作，为泰安网络安全产业发展打下坚实的人才基础。

重庆合川打造信息安全产业城。2019年6月，360网络安全协同创新产业园一期项目开工建设，总面积约7000平方米，整体工程预计将在7月底前基本完成，8月底前全面建成投用。

四川成都网络信息安全产业园获得增资。2018年4月，中国电科（成都）网络信息安全产业园获得增资，目前总投资超过500亿元。此次增资将有助于进一步为大数据安全、云安全等新兴产业发展提供保障，并加强网络安全产业合作。

2．网络安全投资融资活动持续活跃

一是中国互联网投资基金重点关注网络安全、人工智能、“互联网+”、大数据、云计算等重点创新领域和业务模式。2018年8月1日，中网投D轮投资恒安嘉新；2019年6月28日，中网投作为战略投资者入股北京梆梆安全科技有限公司。**二是**创投机构密集围绕网络安全领域开展布局。苹果资本专注全球网络安全产业项目，截至2019年，苹果资本已投资超过三十家企业，并在2018年分别联合昆仲资本、高成资本等对全知科技和指掌易实现上千万和2亿人民币投资。2018年北极光创投对云屏科技进行2000万人民币天使轮投资，联合联想创投等对云杉网络进行1100万美元投资，联合元禾资本等对山

石网科进行战略投资。CBC[67]宽带资本则对几何安全进行战略投资，联合红杉资本等对青藤云进行 2 亿元人民币投资，并于 2019 年领投芯盾时代实现 3 亿元人民币投资。

3．协会联盟推动增进产业自律协同

一是强化网络安全服务能力评定。中国通信企业协会网络安全专业委员会积极开展网络安全服务能力评定工作，目前已有 92 家网络安全企业取得了风险评估、设计集成、应急响应、安全培训等 154 个网络安全服务能力资质。**二是**联合开展网络安全前瞻研究。2019 年中国网络空间安全协会组织近 10 余次座谈研讨，研判网络安全态势、技术走向、投融资趋势，研究网络空间立法、制度建设等重要问题。**三是**搭建企业国际拓展的桥梁。中国网络安全产业联盟与中关村管委会合作，积极组织会员单位参加第三届中俄网络安全产业圆桌会议、RSAC2019[68]、Trustech2019[69]和 CYBER TECH[70]等国际会议，其中 RSA2019 有 36 家中国企业参展，相比去年增加了 38%。

4．网络安全人才队伍建设加快推进

一是网络安全竞赛演练如火如荼。2018 年 8 月，“护网杯”—2018 年网络安全防护赛暨首届工业互联网安全大赛开赛，共有近 3000 支队伍报名参赛。12 月，第五届电信和互联网行业网络安全技能竞赛决赛在京举行，近千名选手参加，最终评选出优秀个人 165 位、优秀团

[67] CBC：China broadband capital，中国宽带资本
[68] RSAC2019：2019 RSA Conference，2019 RSA 信息安全大会
[69] Trustech2019：2019 法国智能卡展
[70] CYBER TECH：世界网络安全大会

队 55 个。2019 年 6 月，围绕关键信息基础设施的实战攻防演习“护网 2019”圆满完成，演习以检验关键信息基础设施和重点网站网络安全的综合防御能力和水平为主要目标，构建了多层次多渠道合作。**二是**联合实验室加紧搭建。2019 年 4 月，中国信通院联合中国移动等成立“物联网安全创新实验室”，促进物联网安全创新技术、产品孵化和能力提升；7 月，联合腾讯安全成立“产业互联网安全实验室”，围绕人工智能、区块链、云计算等领域开展务实合作。**三是**安全会议活动规模空前。2018 年 9 月，2018 年国家网络安全宣传周在成都成功举行，其中，网络安全博览会 5 天总参观人数达 7.5 万人次。2019 年 8 月，2019 北京网络安全大会成功落下帷幕，会议聚集了 20 位两院院士、400 多位国内外安全领袖和 80 余家参展机构。

（五）网络安全国际合作持续深化

1. 网络空间国际交流合作日益紧密

一是交流协作载体不断丰富。金砖国家未来网络研究院中国分院在深圳揭牌，重点开展新型网络体系架构、新一代移动通信、工业互联网、人工智能、车联网、网络与信息安全等领域国际合作。360 与以色列签署了战略合作协议，成立中以网络安全科技创新中心，组建 360 以色列网络安全产业发展基金，并建设中以网络安全技术协同创新产业园。**二是**技术共享合作纵深发展。中国网安与卡巴斯基签署战略合作备忘录，深化工控安全、威胁情报、安全培训等方面合作，并

轮值举办中俄网络空间安全“T3”国际论坛。奇安信与以色列 Cyberbit[71] 公司达成战略合作，双方将通过整合各自的技术优势和产业资源，为国内政企客户和高等院校深度定制网络空间安全人才培养和网络攻防靶场解决方案。**三是**投资并购活动有序展开。华为收购了以色列数据库安全公司 HexaTier 和基于软件的系统设计和芯片设计公司 Toga Networks，相关能力纳入华为下一代网络和企业安全产品组合。

2．国内企业国际化探索纵深推进

近年来，越来越多的国内网络安全企业制定了面向全球的发展战略，努力开拓海外网络安全市场。**一是**部分企业实现海外扩展取得成效。**一方面**，海外营收持续增长，截至 2018 年 12 月，深信服海外营收规模为 1.05 亿元，较 2017 年增长 76.81%；飞天诚信海外营收规模为 1.31 亿，较 2017 年增长 7.26%。**另一方面**，海外研发中心加快建设，360 在美国加利福尼亚州设立研发中心，深信服、山石网科、绿盟等则在硅谷进行布局。**二是**“一带一路”成为国际化布局重要方向。启明星辰与中国友谊促进会签署战略合作协议，将共同服务于“一带一路沿线国家的网络基础设施的安全保障；上海观安将为古巴、委内瑞拉和萨摩亚等“一带一路”沿线国家提供网络安全培训；奇安信与印尼 AG 集团达成合作，将共建威胁感知基础设施平台。**三是**国际网络安全大会仍是国际化拓展的重要平台。2019 年美国 RSA 大会上，中国参展机构达到了 36 家，较 2017 年增长了 38%，全面展示了我国企

[71] Cyberbit：位于以色列，安全公司

业在云安全、工控安全、大数据安全、终端安全、身份管理与访问控制等领域的网络安全解决方案。

三、重点细分领域技术发展进展

（一）工业互联网安全生态加速构建

1．现状：工业互联网安全产品和服务体系初步建立

随着工业互联网、物联网、云计算、移动互联网等技术的深入发展，IT[72]与 OT 加速融合，工业体系逐渐由封闭走向开放，网络安全威胁开始向工业环境渗透，工业互联网安全问题日益凸显，市场需求随之攀升。工业互联网安全产品形态与传统网络安全产品相近，但在具体技术实现上具有工业领域的特殊性，包括需要支持多种工业协议、满足业务生产的高可靠低时延要求等。**在工控系统（OT 网络）方面，边界和终端安全防护仍是主要手段**。OT 边界安全通常由部署在 OT 网络和 IT 网络之间控制区内的防火墙、入侵检测、单向网关等设备或采用软件定义的方式实现，终端安全与 IT 领域类似。Veracity Industrial Networks[73]的 Cerebellum 平台通过软件定义网络架构提供包括安全级模型构建、授权网络设备管理、安全域管理、通信授权、可视化验证、安全策略管理等功能。国内厂商工业互联网安全相关产品线日益完备，中国网安的工业防火墙支持 Modbus/TCP[74]、PROFINET[75]、

[72] IT：Internet Technology，互联网技术
[73] Veracity Industrial Networks：位于美国加利福尼亚州，工业安全公司
[74] Modbus/TCP：一种工业以太网协议
[75] PROFINET：基于工业以太网技术的自动化总线标准

Siemens S7[76]、FINS[77]等 10 余种工控协议，可有效抑制病毒、木马威胁在工控网安全区域间的传播和扩散；威努特基于对工业控制协议的深度解析（DPI[78]），结合“白名单+智能学习”机制，对各类工控协议进行快速捕获和指令级解析；启明星辰通过对工控系统重要区域内节点间的通信流量检测，发现工控系统中存在的异常行为和潜在威胁。**在工厂 IT 网络和工业云方面，工业互联网安全监测与态势感知能力建设成为趋势**。工厂 IT 网络和工业云平台相对 OT 网络更为开放，也更容易遭受网络攻击。工业互联网安全监测和态势感知是一种基于工业环境，动态、整体地洞悉安全风险的能力，从全局视角对安全威胁进行发现识别、理解分析和响应处置。Cyberbit 的 SCADA Shield 综合网络安全产品能够自动发现网络中设备，识别配置异常，基于深度包检测技术识别协议每一层中需要分析的特定字段进行 OT 网络监视，从而提供态势感知能力；上海观安通过部署探针、网关等关键设备，对工业互联网平台、工业互联网应用设备和系统、企业内外网等的安全运行情况进行监测与感知，同步构建技术手段汇集来自各方的工业互联网安全态势信息，综合形成全天候、全方位态势感知能力；360 工业互联网安全大脑系统通过感知、决策、响应三种手段形成整套智能安全系统，基于 ICS[79]全网资产扫描、从 IT 系统到 OT 系统总线感知、内网数据与外网情报交叉分析等手段，实现实时数据上报和动态

[76] Siemens S7：一种西门子通信协议
[77] FINS：factoryinterface network service，欧姆龙公司开发的通信协议
[78] DPI：Deep packet inspection，深度报文解析
[79] ICS：Industrial control system，工业控制系统

策略部署，阻断攻击行为。**工业领域的安全检测评估与安全培训等服务逐步升温。**近年来，工业领域安全事件频发，不断敲响网络安全警钟。2017 年，“永恒之蓝”蠕虫病毒入侵了全球 150 多个国家的信息系统，多家汽车制造商被迫停产，能源与通信等重要行业损失惨重；2018 年，台积电多个工厂及营运总部遭遇勒索软件攻击，导致在台湾北、中、南三处重要生产基地生产线停摆；2019 年挪威海德鲁铝业公司遭“LockerGoga”勒索攻击，多工厂关闭。工业领域网络安全意识逐步提升，开展安全评估、防范安全风险、培育工业领域安全人才等任务和需要日益迫切，带动安全服务市场需求稳步增长。国内部分工业互联网安全厂商能力介绍如表 5 所示。

表 5　国内部分工业互联网安全厂商能力介绍

类别		360	上海观安	中国网安	天地和兴	天融信	安天科技	威努特	亚信安全	启明星辰	安恒信息	杭州迪普	奇安信
协议支持情况		支持Ethernet/IP、Modbus/TCP、OPC等10余种工控协议深度解析	支持30多种主流工控协议解析	支持30余种工业协议深度解析	预置40种工业协议及种用IT通协议;支持不少种控议多网用的别工业协制和60IT通协络协识	支持Modbus TCP、OPC、IEC 60870-5-104、Siemens S7等几十种工控协议解析	支持10+种主流工控协和HTTP、FTP、SMTP、POP3、IMAP、DNS等200余种协传统协议	支持OPC、Siemens S7、Modbus、IEC104、Profinet、DNP3等多种协工控议深度解析	支持协议数超过100余种,可所口侦测端及余种通讯的应用	支持预种工议,支置百见协持工议义常业协定业支自	支持Modbus、S7、HTTP、FTP等35种协议报文解析,20种工控协议深析度解	支持百业并种工议自定协可义扩展,支持TCP和ICMP等协议检状态测	支持23种IT/OT协议解析,识别工业协议40+种、应用协议3000+以上
安全防护类	主机防护产品	√		√	√	√	√	√	√	√	√		√
	工控防火墙	√		√	√	√		√	√	√	√	√	√
	工业网闸	√		√	√	√				√			√
	入侵检测产品	√		√	√	√	√	√	√	√	√	√	
	漏洞扫描工具			√		√		√	√	√	√	√	
	检查评估工具			√	√	√	√	√	√	√		√	√
	敏感数据保护			√		√		√	√	√			
	其他	USB安全隔离系统			APT检测、堡垒机	病毒过滤网关等						异常流量清洗系统	

类别		360	上海观安	中国网安	天地和兴	天融信	安天科技	威努特	亚信安全	启明星辰	安恒信息	杭州迪普	奇安信
运营监测类	安全审计	√	√	√	√	√		√	√	√		√	√
	工控安全监测系统	√	√	√	√	√		√	√	√	√	√	√
	安全态势感知平台	√	√	√	√	√	√	√	√	√	√	√	√
	蜜罐	√	√										
	安全管理系统	√				√							
	其他	信号感知系统				网站安全监控系统	威胁捕获系统		安全认证平台				
工业设备类	安全交换机			√								√	
	其他	安全通信模组											
安全服务类		√		√	√	√	√			√			

数据来源：中国信息通信研究院根据公开资料整理

2．展望：工业互联网安全步入发展战略机遇期

日趋频繁的网络攻击事件和持续加码的政策要求为提升工业企业安全意识、推动工业互联网安全能力建设提供了良好契机。**一是**工业互联网安全政策导向增强，形成对网络安全市场的带动力。2019 年 7 月，工业和信息化部等十部门联合印发《关于印发加强工业互联网安全工作的指导意见的通知》，提出“加强工业生产、主机、智能终端等设备安全接入和防护，强化控制网络协议、装置装备、工业软件等安全保障”、“工业互联网平台的建设、运营单位按照相关标准开展平台建设，在平台上线前进行安全评估”、“建立健全工业 APP 应用前安全检测机制，强化应用过程中的用户信息和数据安全保护”等系列要求，为工业互联网安全能力建设指明方向。**二是**以 IT 视角为主的安全产品和服务难以满足工业互联网的实际需求，工业互联网安全仍需突破瓶颈，面向 OT 纵深发展。根据 Gartner 统计，2018 年，10%以资产为中心的企业采用将传统安全与专业 OT 安全技术混合部署模式来保护 OT 环境，这一比例将在 2022 年达到 30%。在特殊性能需求方面，工业互联网需要保障生产的连续性和可靠性，IT 网络中常见的影响网络时延或开销的操作在 OT 网络中可能无法适用，提供平衡安全风险和业务影响的方案将成为工业互联网安全厂商追求的目标。在网络复杂度方面，IT 网络中的资产管理模式难以适应 OT 网络中混合的生产协议、未知资产、遗留系统和设备，IT 网络中的安全方法也不适配于工业互联网行业垂直性强的特性，支持更多的工业控制协议

的细粒度解析，正确标识与管理 OT 资产、充分挖掘和使用垂直威胁情报都将成为工业互联网安全发展的重要方向。**三是**工业领域网络安全宣传教育亟需加强。人是安全的尺度，通过培训提升 OT 人员的安全意识和技能，将是最快最有效的网络安全风险规避方式。

（二）云安全发展态势持续向好

1．现状：云安全市场保持强劲增长

云计算作为信息技术发展和服务模式创新的集中体现，是推动互联网、大数据、人工智能和实体经济深度融合的基石。近年来，伴随云计算技术广泛普及，云安全问题日益受到重视，云安全市场持续快速增长。根据 Gartner 数据，2018 年全球云安全软件市场规模达到 58.09 亿美元，相比 2017 年增长 18.4%[80]；Forrester[81]预测，2023 年云安全支出将增长至 126 亿美元。国内外安全厂商持续加大力度布局，2019 年 RSAC700 多家参展企业中，近 42%提供云安全产品和解决方案。

公有云方面，云安全技术创新活跃，风险监测防御、应对多云环境、敏感数据保护等仍然是云安全热点领域。**在云工作负载保护平台（CWPP[82]）方面**，Symantec 的 CWPP 产品基于内置云原生适配器适应 AWS[83]、Azure[84]和 Google[85]云等不同云计算环境，自动探测可用域、

[80] 数据来源：Gartner，Forecast: Public Cloud Services, Worldwide, 2017-2023, 2Q19 Update
[81] Forrester：技术和市场调研公司
[82] CWPP：Cloud Workload Protection Platform，云工作负载保护平台
[83] AWS：Amazon Web Service，亚马逊公司旗下云计算服务平台
[84] Azure：微软公司旗下云计算服务平台
[85] Google：谷歌公司，成立于 1998 年，全球最大的搜索引擎公司

标签、网络等云计算环境信息作为策略和告警模块的上下文信息补充，并通过安装代理实现漏洞管理、实时恶意软件保护等功能；Radware[86]结合沙箱技术和加密挖矿控制套件，采用自动检测和自动响应来识别、警告和阻止公有云中的加密劫持挖矿活动；青藤云基于自适应安全架构构建云上防护平台，为用户提供持续监控、分析及响应；椒图科技采用 RASP[87]、ASVE[88]、沙盒等基于异常行为的检测技术，检测并防御未知威胁。**在云访问安全代理（CASB）方向**，国外主流厂商均已推出 CASB 产品或解决方案，如微软、Netskope[89]、Bitglass[90]、Skyhigh[91]等；国内 CASB 市场仍处于萌芽阶段，奇安信产品云守基于对特定云应用的数据安全防护策略保障云端数据及网络安全，对云端和传输中的数据通过认证、标记化和加密等方式进行保护，产品内置 AES[92]算法、中国标准国密 SM 算法等数十种算法，保证结构化及非结构化数据安全；臻至科技通过使用深度学习技术按需监控相关应用及软件实现 CASB 能力，提供 AES-GCM 256 位加密算法、针对 ARM[93]平台的 CHACHA20 算法以及流式加密等，并支持将所有密钥部署在全球区块链节点上。**在容器安全方向，**Aqua[94]的 Cloud Native Security Platform 产品提供了针对容器和无服务环境的综合型安全管理平台，包括基于

[86] Radware: 总部位于以色列特拉维夫市，智能化解决方案供应商
[87] RASP：Runtime application self-protection，运行时应用自我保护
[88] ASVE：Application security virtual environment，虚拟化安全域
[89] Netskope：成立于 2012 年，云端应用监控服务商
[90] Bitglass：位于美国加利福利亚，云安全初创公司
[91] Skyhigh：云安全公司，2017 年被迈克菲(McAfee)收购
[92] AES：Advanced Encryption Standard，密码学中的高级加密标准，又称 Rijndael 加密法
[93] ARM：Advanced RISC Machine，一款 RISC 微处理器
[94] Aqua：成立于 2015 年，容器及微服务安全公司

CI/CD[95]环境扫描的漏洞管理功能、针对 PCI DSS[96]等标准和法案的合规审计服务以及其他相关安全能力；目前国内在容器安全方向仍处于实验研究阶段。**在数据防泄漏（DLP[97]）方向，**McAfee[98]的 MVSION Cloud 产品对云中数据实施防泄漏策略，自动对敏感信息进行分类，以便在云中进行删除或隔离；思睿嘉得使用机器学习、自然语言处理、文本聚类分类等技术实现数据分类分级，使用 ORC[99]和图片相似度实现图像内容识别，支持终端策略阻断、互联网外发阻断、邮件审批等数据保护功能。

私有云方面，除云工作负载保护平台、数据防泄漏等公私有云均适用的产品外，国内厂商聚焦于以云安全资源池为核心的云安全综合解决方案。云安全资源池提供虚拟化的安全能力，如防火墙、WAF、IDS、IPS、堡垒机、数据库审计等，并通过统一安全管理平台对各类安全能力进行组织和编排，形成整体安全方案。安恒信息通过为用户提供包含云监测、云防御、云审计等覆盖全生命周期的云安全产品服务提供一站式云安全解决方案；启明星辰则运用虚拟化、软件定义安全等技术提升安全资源的利用效率并形成各项安全能力的动态编排以及实现云上引流。国内部分云安全厂商能力介绍如表 6 所示。

[95] CI/CD：Continuous Integration/Continuous Deployment，持续集成/持续部署
[96] PCI DSS：Payment Card Industry Data Security Standard，第三方支付行业数据安全标准
[97] DLP：Data leakage prevention，数据防泄漏
[98] McAfee：迈克菲，总部位于美国加州圣克拉拉市，计算机安全解决方案厂商
[99] ORC：optical character recognition，光学文字识别

表 6　国内部分云安全厂商能力介绍

类别		360	山石网科	中国网安	天融信	亚信安全	启明星辰	安恒信息	迪普科技	奇安信	腾讯	深信服
采用云资源池技术方案		√		√	√	√	√	√	√	√		√
网络安全	DDoS 防御	√		√		√			√	√	√	√
	云防火墙	√	√	√	√	√	√	√	√	√		√
	IDS	√				√	√					
	IPS	√		√		√	√					
	VPN			√	√							
	网络/流量审计						√		√			
	其他			数据交换隔离网关			超融合检测					
主机安全	主机安全	√		√		√	√	√		√	√	√
	病毒查杀					√						
应用安全	WEB 应用防火墙	√	√	√	√	√	√	√	√	√	√	√
	网站威胁扫描	√	√	√	√	√		√	√	√	√	√
	网页防篡改	√	√	√			√	√	√	√		√
	其他								爬虫防护			

类别		360	山石网科	中国网安	天融信	亚信安全	启明星辰	安恒信息	迪普科技	奇安信	腾讯	深信服
接入安全	CASB			√								√
业务安全	内容安全			√					√		√	√
数据安全	数据加密			√			√				√	
	数据库审计	√	√		√		√	√		√	√	√
	数据防泄漏		√				√				√	√
	云数据备份										√	
	其他			数据安全监管平台								
安全管理	云安全态势管理	√		√		√				√	√	√
	密钥管理			√		√					√	
	堡垒机	√			√	√	√	√		√	√	√
	SSL 证书管理			√								
	漏洞扫描	√			√		√					
	安全审计	√			√		√					
	基线管理				√		√					
安全服务	安全专家服务	√		√		√		√	√	√	√	√

数据来源：中国信息通信研究院根据公开资料整理

2．展望：政策红利与技术革新驱动云安全高质量发展

云安全政策标准的发布实施和云计算市场的快速扩张将共同推进云安全市场再上新台阶。**一是**安全合规的持续强化将进一步激发云安全需求。2019 年 5 月，国家标准《信息安全技术 网络安全等级保护基本要求》（“等保 2.0”）正式发布并将于年底实施，标准新增“云计算安全扩展要求”，进一步提出不同等级云计算平台的安全扩展要求；7 月，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部共同发布《云计算服务安全评估办法》，以提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平。云安全政策标准的进一步细化完善，将进一步提高云租户等对云安全的重视程度，有效带动云安全市场需求。**二是**支持多云的安全解决方案、云内东西向安全或将成为发展重点。多云模式可以提供针对不同业务场景和安全需求的解决方案，降低企业上云成本，提高云计算环境的数据业务安全性以及抗灾能力。多云的部署发展，将驱动适配多云模式的安全解决方案需求增长。随着云计算规模扩大和云中节点数增加，云内渗透威胁亦逐渐加剧，CWPP、微隔离、终端防护等东西向防护技术和产品需求日益迫切。**三是**云计算技术的发展将进一步推动云安全技术创新。近年来，云计算技术发展迅速，容器、微服务、云原生、DevOps[100]等新兴技术已逐渐成为云计算技术的新方向，

[100] DevOps：Development 和 Operations 的组合词，是一组过程、方法与系统的统称，用于促进开发（应用程序/软件工程）、技术运营和质量保障（QA）部门之间的沟通、协作与整合

相关安全挑战也随之产生，容器安全、DevSecOps[101]等技术成为云安全领域的研究热点。此外，随着 5G、物联网、区块链等新技术的发展，云计算环境将面临新的安全挑战，从而催生新的云安全需求。

（三）零信任从“概念”走向落地

1．现状：零信任安全框架落地实践逐步增加

近年来，“零信任”日益成为各国网络安全企业高度关注、抓紧布局的新领域。2010 年，咨询公司 Forrester 分析师约翰·金德维格首次提出“零信任模型”，在“所有网络流量都不可信”的基础上，要验证并保护所有来源、限制并严格执行访问控制、检查并记录所有网络流量日志。2018 年，Gartner 提出，零信任是实践持续自适应的风险和信任评估（CARTA[102]）的第一步。零信任以默认拒绝的方式开始，认为需要认证一切，按需对不同身份（设备、用户和网络流量）授予区别化和最小化的访问权限，并通过持续认证改变“通过认证即被信任”的防护模式。国内外企业基于对零信任安全框架的理解，开展了技术探索和布局，目前多用于解决身份管理和访问控制的问题，聚焦于软件定义边界（SDP[103]）、微隔离等方向。**软件定义边界凭借更细粒度的控制、更灵活的扩展、更高的可靠性，正在改变传统的远程连接方式。**谷歌的 BeyondCorp 基于设备、用户、动态访问控制和行为感知策略实现其零信任构想，所有流量通过统一的访问代理来实现认证和授权，

[101] DevSecOps：一种安全理念，从 DevOps 的概念延伸和演变而来，核心理念为安全是整个 IT 团队（包括开发、运维及安全团队）每个人的责任，需要贯穿从开发到运营整个业务生命周期的每一个环节

[102] CARTA：continuous adaptive risk and trust assessment

[103] SDP：Software Defined Perimeter，软件定义边界

实时更新指纹库中的用户、设备、状态、历史用户行为可信度等相关信息，利用动态的多轮打分机制对请求来源进行信任层级划分，从而进一步实现层级内的最小权限控制；思科将 Duo Security、Tetration、SD-Access 能力有机结合，推出了面向工作人员、工作负载、工作场景的零信任安全方案；Cyxtera[104]推出了 AppGate SDP 方案，遵循以身份为基石、零信任模型、为云而建像云一样三大原则；Verizon[105]推出了 SDP 服务，并购买 Vidder[106]公司基于 SDP 的 PrecisionAccess 解决方案，完善零信任整体布局；云深互联的访问控制网关依据最小权限原则按需授权，实现动态访问控制、访问监控、访问追踪等功能，同时其 SDP 方案利用动态端口技术，隐藏企业安全边界出入口。**微隔离技术实现对工作流级别的细粒度隔离和可视化管理，正在成为虚拟化环境下网络隔离优选方案**。Illumio[107]的自适应安全平台以微隔离技术为基础，在隔离策略配置方面，应用人工智能学习网络流量模式，提供多种便捷配置模式和可视化展示。蔷薇灵动的微隔离产品基于主机代理实现自适应安全防护，以主机和负载作为对象进行访问控制，实现大规模网络的东西向防护。山石网科的云•格产品可基于云网络 4-7 层实现最低授权控制策略，提供开放 API[108]，支持资产发现识别、策略自动绑定、自动化部署。

[104] Cyxtera：总部位于美国，安全公司
[105] Verizon：威瑞森通讯，无线运营商
[106] Vidder：物联网安全公司
[107] Illumio，成立于 2013 年，网络安全初创企业
[108] API：Application Programming Interface，应用程序接口

目前，国内企业逐步加大对“零信任框架”的研究和布局，奇安信、腾讯、蔷薇灵动、山石网科、九州云腾、云深互联、芯盾时代等开展了系列探索和实践。国内部分零信任安全企业实践如表 7 所示。

表 7 国内部分零信任安全企业实践

企业名称	技术领域/特点
山石网科	• 将下一代防火墙安全服务能力下沉至云计算环境中各宿主机内； • 在 OpenStack[109]、VMware 环境中实现软件定义安全； • 提供基于 SDN[110]的网络微隔离、可视化安全解决方案。
云深互联	• 旨在通过新一代 SDP 网络隐身技术使得企业应用只对授权用户可见； • 深云 SDP 由三大组件构成：深云 SDP 安全大脑、深云隐盾网关、深云 SDP 客户端； • 主要优势为网络隐身、按需授权、态势感知等。
九州云腾	• 专注于“云大物移”领域统一身份认证管理； • 使用 Docker[111]微服务架构，采取 OpenID Connect[112]机制，支持 Fido[113]等 10 多种开发者认证协议。
芯盾时代	• UEBA[114]产品与 IAM[115]产品融合，通过身份认证、业务行为分析、自动化响应、风险调查，打造内部零信任业务安全平台； • UEBA 产品可以单独部署。
蔷薇灵动	• 致力于为虚拟化数据中心提供领先的网络安全管理产品和服务； • 使用代理技术提供兼容混合云的微隔离服务； • 主要能力在于为数据中心提供东西向流量的可视化与自适应管理。
奇安信	• 实现以身份为基石、业务安全访问、持续信任评估、动态访问控制四大核心特性； • 由可信环境感知、可信应用代理、可信 API 代理、可信访问控制台、智能身份分析系统、智能身份平台等核心产品组件构成。
腾讯	• 采用多种认证方式，确保访问来自可信用户。

数据来源：中国信息通信研究院根据公开资料整理

[109] OpenStack：开源的云计算管理平台项目
[110] SDN：Software Defined Network，软件定义网络
[111] Docker：开源应用容器引擎
[112] OpenID Connect：基于 OAuth 2.0 协议的轻量认证级规范
[113] Fido：Fast Identity Online，线上快速身份验证联盟
[114] UEBA：user and entity behavior analytics，用户实体行为分析
[115] IAM：Identity and Access Management，身份识别与访问管理

2．展望：技术变革驱动零信任安全创新前行

网络技术的变革为零信任安全提供了变革的温室和全新的挑战。**一是基于零信任理念的探索实践将持续深化。**目前国内零信任还在初步探索，相应技术、产品和实践均处于萌芽阶段。随着云计算、大数据、微服务、移动网络等技术的发展，移动成为设备、业务和人员的基本属性，网络“内部”和“外部”边界区别也逐渐模糊，传统基于网络边界的防护模型在新网络态势中不再适用，基于零信任模式的需求将逐步增加，对零信任理念的理解也将在实践中逐渐深化。**二是基于零信任的身份管理实践将从边界侧开始，逐步深入业务运营，最终构建完整体系。**传统身份认证主要在网络边界侧实现，而随着内外网边界的逐渐模糊，网络内部的认证手段缺乏问题将逐渐暴露，内网防护需求日益增强。在当前的安全环境中，业务内部的身份认证需要业务的改造以及平台侧的配合，实现难度和改造成本较高，而在国内业务上云、5G 等趋势推动下，业务模式转换和迁移将为零信任理念提供实践的平台，从而充分利用内部业务、数据、设备等信息，形成持续、动态和细粒度的零信任防护方案。**三是随着零信任理念与传统技术的深度融合，新型身份管理和访问控制解决方案有望加速实践落地。**零信任身份管理不代表完全抛弃传统身份管理与访问控制技术，传统安全厂商应积极拥抱网络技术和安全理念的变革，将零信任理念与传统鉴权、授权、审计等技术融合，发挥传统安全厂商在身份管理领域的深耕优势，开展新技术研究与相关产品开发，划清传统理念与新理

念的异同点和边界，降低技术与产品变更成本。

（四）人工智能与网络安全加速融合

1．现状：人工智能赋能网络安全效用日益显现

人工智能技术在数据分析、知识提取、智能决策等方面的优势为应对动态多变、复杂交织网络安全问题提供了新思路，网络安全已经成为人工智能应用的重要方向之一。根据法国咨询机构凯捷 2019 年 7 月发布的《以人工智能重塑网络安全》报告，超过半数的被调研企业认为实施基于人工智能的网络安全措施势在必行。美国咨询机构 CB Insights[116]统计数据显示，2018 年至 2019 年 6 月间，与网络安全相关的人工智能投融资活动超过 180 笔。以大数据分析、机器学习、深度学习、人机协同为代表的人工智能与网络安全融合实践日益增多。**在异常流量检测方面，人工智能为加密流量分析提供新方案**。思科已将 AI 驱动的加密流量分析应用于交换机等产品，基于初始数据包特征以及后续数据包长度与时序等，通过机器学习算法识别异常流量，提供加密流量检测能力；Darktrace[117]基于无监督学习算法构建核心异常检测算法体系，为网络中用户和设备建立行为模型以区分正常模式和攻击行为，并对攻击进行标记和阻止，在此基础上提供企业免疫系统、工业免疫系统等产品；观成科技推出针对恶意加密流量的 AI 检测引擎，通过人工智能算法训练加密流量检测模型，支持 SSL[118]、

[116] CB Insights：CB Insights，全球知名创投研究机构
[117] Darktrace：创立于 2013 年，英国网络安全初创公司
[118] SSL：Secure Sockets Layer，安全套接字层

SSH[119]、RDP[120]等多种加密协议分析。**在恶意软件防御方面，针对特定场景人工智能应用取得积极进展。**Agari[121]面向电子邮件业务开发了智能检测功能，防范针对邮箱的钓鱼攻击和恶意访问；Cylance[122]利用机器学习算法基于文件特征识别恶意软件，在勒索病毒防御方面效果突出；芯盾时代针对金融反欺诈场景推出智能行为认证产品，基于异常检测及样本标注、欺诈关联图谱等持续发掘欺诈新模式。**在异常行为分析方面，人工智能正成为模式识别的有效补充。**Exabeam[123]的核心产品安全信息和事件管理（SIEM）平台，通过分析公司的日志数据创建异常检测模型，实现异常活动识别和风险评估；Securonix[124]的下一代 SIEM 产品基于 Hadoop[125]构建可扩展的大数据分析架构，提供日志管理、用户和实体行为分析功能，通过人工智能算法检测高级攻击并实现应急响应；启明星辰的 UEBA 产品在对多源异构数据归一处理基础上，利用机器学习等技术建立用户和实体对象行为正常基线并监测与基线的偏离；瀚思科技的 UEBA 解决方案聚焦于对企业内部员工的异常行为进行定位，结合审计、溯源、DLP 等企业原有安全能力，提高检测效果。**在敏感数据保护方面，人工智能助力数据识别和保护能力提升。**亚马逊推出 Amazon Macie Analytics 服务，可通

[119] SSH：Secure Shell，安全外壳协议
[120] RDP：Remote Desktop Protoco，远程桌面协议
[121] Agari：位于美国加利福尼亚州，电子邮件安保公司
[122] Cylance：创立于 2012 年，位于美国西海岸
[123] Exabeam：创立于 2013 年，网络安全初创公司
[124] Securonix：创立于 2008 年，安全分析厂商
[125] Hadoop：由 Apache 基金会所开发的分布式系统基础架构

过机器学习技术自动识别重要数据访问、复制、移动等可疑行为，并实施准实时的修复措施，防范重要数据暴露及共享业务中的数据安全风险；德国 Neokami[126]推出了 CyberVault 产品，可利用人工智能发现、保护和管理云端和本地的敏感数据；亚信安全的数据分类分级发现系统在数据块维度多任务并行处理，利用机器学习+语义分析生成训练模型提高数据分类速度和精度，提供数据特性及变化趋势展示。**在安全运营管理方面，安全编排与自动化响应（SORA[127]）逐渐兴起。**IBM[128]推出 Resilient 事件响应平台，可提供响应流程定制功能，灵活编排响应活动并自动审计跟踪，实现对威胁事件的快速响应；Palo Alto Networks 于 2019 年 2 月收购了 Demisto[129]，并随即于 3 月推出人工智能安全平台 Cortex，Cortex 数据湖致力于打破网络、云端、终端数据孤岛，并支持对海量数据分析、威胁发现及响应策略快速编排，目前 PwC[130]、Critical Start[131]、On2it[132]、TrustWave[133]等厂商已通过 API 方式接入该平台并提供安全能力；安恒信息的 AiLPHA 大数据智能安全平台结合智能关联分析引擎，构建规则模型、统计模型、机器学习模型和无监督的聚类分析，并通过“AI 安全大脑”对企业安全要素进行智能编排，实现威胁管理流程的自动化建模。国内企业应用人工智

[126] Neokami：创立于 2014 年，位于德国
[127] SORA:：Security Orchestration, Automation and Response，安全编排与自动化响应
[128] IBM：International Business Machines Corporation，国际商业机器公司，总公司在纽约州阿蒙克市
[129] Demisto：创立于 2015 年，位于美国加利福利亚州库比提诺
[130] PwC：普华永道，全球顶级会计公司，在安全咨询业务领域占据着领先地位
[131] Critical Start：创立于 2012 年，网络安全咨询公司
[132] On2it：创立于 2005 年，位于欧洲
[133] TrustWave：创立于 2007 年，托管安全服务提供商

能赋能网络安全主要实践如表 8 所示。

表 8 国内企业应用人工智能赋能网络安全主要实践

企业名称	技术领域/特点
山石网科	• 基于机器学习的网络流量检测、融合欺骗式检测、关联性分析还原等综合威胁检测技术。
上海观安	• 使用异常检测算法来检测 WEB 异常访问； • 利用时间序列模型（例如马尔科夫链等）和图算法对内网主机行为分析，识别内网主机失陷； • 利用语言模型识别 OWSAP top10 攻击，利用图数据库和图算法溯源。
字节跳动	• 利用深度学习技术加固传统安全防御体系，利用 LSTM 等序列模型构建异常检测方案加强云计算和微服务安全，防范针对深度学习算法和模型的攻击。
微步在线	• 使用远控类型的情报指标、木马协议分析特征分析、基于深度学习算法的 DGA[134]等多种方法进行威胁检测。
阿里云	• 采用自然语言理解算法识别文本垃圾和恶意行为； • 深度学习算法结合独有的情报、舆情、预警和分析体系及实时更新的样本图库，快速定位敏感信息。
默安科技	• 基于深度学习和深度包检测以及深度流检测技术，自动发现所有云资产并进行资产建模。
腾讯	• 使用腾讯优图的 DeepEye 识别技术引擎，对内容进行置信度分析，依托腾讯社交的海量样本优势进行深度识别训练； • 基于多模型匹配技术，识别恶意文本。
深信服	• 利用大数据、机器学习、数据挖掘等技术，建立恶意文件样本库，对恶意 URL[135]、僵尸网络硬编码域名、隐秘隧道通信等进行检测识别。

数据来源：中国信息通信研究院根据公开资料整理

2. 展望：人工智能应用机遇与风险并存

目前，人工智能在网络安全领域的应用仍处于初级阶段。随着研

[134] DGA：Domain Generation Algorithm，域名生成算法

[135] URL：Uniform Resource Locator，统一资源定位符

究探索的不断推进、技术算法的不断成熟，人工智能技术或将打破传统安全的瓶颈与所能解决问题的边界，为网络安全带来全新范式。**一是**攻防演练为人工智能应用训练提供了有效途径。人工智能算法需要足量、高质量的数据持续训练，网络攻击长尾性、情报链不完整、数据共享不充分等成为制约人工智能成熟应用的瓶颈。随着国内攻防演练对抗实战化、场景多样化、参与方多元化发展，网络攻击路线方式等完整攻击链信息逐渐积累，设备系统联动日益紧密，将为人工智能算法训练和模型建立提供了有力支撑。**二是**机器学习依然是智能安全的主攻方向。相对于卷积神经网络等深度学习技术，机器学习技术研究起步早、实践应用多，且多建立在专家智慧基础上，在可解释性、检测分析效率等方面具有一定优势，预计在未来一段时间机器学习技术仍然是人工智能在网络安全领域应用的主要方向。**三是**自动化编排和响应的探索应用前景可期。SOAR 在汇集海量网络设备、终端、流量、数据等情报基础上，构建自动化编排、部署与响应为一体的解决方案，可大幅降低安全人力投入，更好应对网络结构日趋复杂、安全威胁持续多样、防御手段整合度低等挑战。**四是**人工智能自身和应用安全问题不容忽视。人工智能技术在为网络安全提供新理念、新手段的同时，也带来了新的安全风险和挑战。一方面，数据样本污染、识别系统混乱、软件漏洞等安全问题日益显现，人工智能数据样本、算法模型、框架平台等技术自身安全亟待加强。另一方面，人工智能与经济社会各领域的深入融合也会引发新的安全风险，需要前瞻研究安

全措施、标准和手段等，确保人工智能安全发展、可靠应用。

（五）5G 网络安全蓄势待发

1．现状：5G 网络安全研发布局密集展开

5G 是实现万物互联的关键信息基础设施，是经济社会数字化转型的重要驱动力量。目前，全球 5G 研发和产业化进程加速推进，我国工业和信息化部已向四家运营商发放 5G 牌照，5G 正式进入商用部署期。5G 网络的发展也为网络安全产业发展提供了广阔机遇。一方面，5G 网络的快速投建为网络安全产品、服务和解决方案带来了巨大的市场空间，进一步带动网络安全产业结构升级和容量扩张；另一方面，5G 网络引入了网络功能虚拟化、边缘计算、网络功能开放等全新架构和技术，网络中模糊的设备安全边界、开放的端口、集中的控制器和边缘部署节点等都在不断激发新的安全需求。在 5G 网络建设和应用发展安全保障的强大需求推动下，安全企业、运营商、设备厂商等纷纷将 5G 安全作为发展布局的重要战略方向，大力推进 5G 安全技术研究和产品研发。

其中，**网络安全企业大多植根于现有优势领域，探索适应 5G 网络特性、业务特征的安全产品和服务升级**。例如，Gelmato[136]在 2018 年 4 月基于 SafeNet 按需数据保护安全软件服务，推出了针对 5G 网络的新一代云虚拟化网络攻击防护部署方案，通过保护和隔离 5G 网络切片中的虚拟函数和应用程序，实现从核心到多访问边缘的虚拟网

[136] Gelmato：金雅拓，成立于 2006 年，数据安全公司、智能卡厂商

络保护；Palo Alto Networks 在 2019 年初发布防火墙产品 K2，旨在保护蜂窝物联网（Cellular Internet of Things, CIoT）基础设施，支持对 RAN[137]、漫游、SGi[138]和非 3GPP[139]的访问保护。**运营商主要聚焦 5G 网络架构安全解决方案和业务场景安全方案。**例如，韩国 SK 电讯[140]已开始将量子随机数生成器技术（Quantum Random Number Generator, QRNG）应用于 5G 网络的用户认证服务器中，并在首尔和大田之间的 5G 网络和 LTE[141]网络整合量子密钥分发技术，以增强数据传输安全性；中国移动于 2019 年 6 月发布“5G 和背包”产品，配套覆盖网络安全、接入安全业务安全、访问安全等在内的一体化安全解决方案。**设备厂商致力于提供更安全的 5G 设备，并与运营商携手打造面向垂直行业的安全解决方案。**例如，诺基亚贝尔与中国电信携手，构建基于 5G 网络和 5G 终端的端到端 AR[142]公共安全解决方案；爱立信与荷兰皇家电信 KPN[143]合作，探索基于 5G 技术的安全自动驾驶解决方案，为荷兰海尔蒙德汽车园区构建安全的互联协作式自动化交通系统。

总体看来，目前面向 5G 的网络安全产品和解决方案仍处于起步阶段，我国网络安全企业也在积极布局，安博通、恒安嘉新等进行了专项募资，卫士通等申报了国家专项研究，亚信安全、山石网科等开展 5G 网络安全保障和威胁应对手段储备。国内企业 5G 安全领域主

[137] RAN: Radio Access Network，无线接入网
[138] SGi：Short Guard interval，无线数据块短间隔
[139] 3GPP：3rd Generation Partnership Project，第三代合作伙伴计划
[140] SK 电讯：Sunkyoung Telecommunications，韩国最大的移动通讯运营商
[141] LTE：Long Term Evolution，无线数据通信
[142] AR：Augmented Reality，增强现实技术
[143] KPN：Koninklijke PTT Nederland (Royal Dutch Telecom)

要探索如表 9 所示。

表 9 国内企业 5G 安全领域主要探索

企业名称	技术领域/特点
360	• 针对 5G 终端设备安全合规性检测和漏洞挖掘服务。
山石网科	• 基于容器管理模块接口、感知容器业务行为等技术产品，构建容器形态的安全服务，应用于面向 5G 的边缘计算等基于容器的微服务环境。
上海观安	• 智慧医疗设备安全监测平台，通过轻量级仿真系统发现威胁，提供 5G 医疗场景安全防护。
中国移动	• 无人机场景安全解决方案、MIoT[144] DDoS[145]攻击场景解决方案等场景化的 5G 安全解决方案。
微智信业	• 5G 无线网络路测/拨测工具，5GDPI 分析工具，5G 无线网络性能规划、监控及分析工具。
亚信安全	• 针对 5G 核心网提出 5Guard 理念，形成 5G 安全风险预测与治理解决方案。
启明星辰	• 5G 的智能网联汽车信息安全风险监控平台，可基于多种 CAN[146]总线的异常攻击检测模型、V2X[147]神经网络检测能力等，提供 5G 环境下智能汽车的安全检测服务。

数据来源：中国信息通信研究院根据公开资料整理

2. 展望：5G 网络安全期待变革突破

随着 5G 商用部署的加快推进，5G 网络安全能力建设迫在眉睫。虚拟化、切片式、开放化的核心网架构以及 eMBB[148]、uRLLC[149]、mMTC[150]等新兴应用场景对 5G 网络安全提出了更高的要求，倒逼网

[144] MIoT：Mobile Internet of Things，移动物联网
[145] DDoS：Distributed denial of service attack，分布式拒绝服务攻击
[146] CAN：Controller Area Network，控制器局域网络
[147] V2X：vehicle to everything，车对外界的信息交换
[148] eMBB：enhanced Mobile Broadband，增强移动宽带
[149] uRLLC：Ultra-Reliable and Low Latency Communications，低时延高可靠连接
[150] mMTC：massive Machine Type Communications，大规模物联网

络安全能力重构升级。**一是**全新的网络架构和应用场景呼唤整体化的解决方案。在低延时业务领域，基于单点的错误判断、延迟或者失效的预警响应都有可能引发灾难性后果，有效的网络安全防护需要基于更全面的安全洞察、更及时的安全预警和更精准的应急响应。通过多源情报汇聚、深度关联分析、有序应急协作实现安全能力的有机整合，提供整体化的解决方案将会成为 5G 安全需求的新趋势。**二是**虚拟化安全是 5G 安全的核心堡垒。SDN/NFV 等虚拟化技术赋予 5G 按需服务等新特性，也改变了传统网络中基于功能网元物理隔离的保护方式。虚拟化以后，网络配置、网络服务控制、网络安全服务部署等管理功能高度集中于 SDN/NFV 控制平面，成为网络控制的“大脑中枢”，需要构建包括容器安全管理、VNF 安全防护、SDN 控制器安全防护、NFV 基础架构安全防护等由点及面的虚拟化安全防护体系。**三是**云边协同构筑从核心到边缘的安全防线。5G 网络充分利用云化技术部署集中化、大区化核心网，同时为支持低时延业务场景，采用边缘计算等技术将核心网控制功能下沉至网络边缘。因此也带来了云端和边缘的安全协同，以及将安全特性和功能直接嵌入边缘的安全新需求，以充分保障云平台、边缘计算平台、接入终端和应用安全，实现从核心到边缘的全程访问保护。

四、我国网络安全产业前景展望

（一）政策红利持续释放有望激活产业动能

一是产业发展顶层设计加强，产业发展重点和方向更为明确。中

央网信办、工业和信息化部等相关部门加强网络安全产业发展统筹规划，积极推进网络安全产业发展纲要性、指导性文件编制，围绕网络安全产业范畴、技术短板、发展方向、政策需求等的调研和研讨密集展开，有望明确规范产业范畴分类，指引网络安全技术产业创新方向。**二是**国家级产业园区加快建设，集群发展效应即将释放。武汉、北京、天津、成都、长沙等全国多个城市大力推进网络安全集聚发展，制定实施了一揽子优惠措施，聚焦网络安全产业发展关键环节、网络安全技术核心短板，搭建产业发展协作平台，聚合网络安全企业、网络运营商、高校、科研机构、金融机构等各方，协同打造“政产学研用”一体化网络安全产业发展生态。

（二）合规需求持续增强助力拓展市场空间

一是网络安全责任意识加强，履职尽责任务迫切。各行业、各领域加紧网络安全责任制度建设，明确各相关方工作职责和措施，规定了未能正确履行网络安全工作职责的问责情形、问责原则和问责程序，为推进网络安全工作提供有力依据。2019 年 4 月，《中央企业负责人经营业绩考核办法》正式施行，提出“违反国家法律法规和规定，导致发生较大及以上网络安全事件，要按照有关规定对相关负责人进行责任追究”，有助于进一步强化和落实网络安全工作责任。**二是**等保关保实施在即，标准规范细化落地。《关键信息基础设施安全保护条例》《网络安全等级保护条例》即将出台，相关措施要求正逐步明确。2019 年 5 月，《信息安全技术网络安全等级保护基本要求》等多项国

家标准（“等保 2.0”）正式发布，提出主动防御、安全可信、动态感知、全面审计等新理念，覆盖云计算、大数据、物联网、移动互联和工业控制系统等新领域，有望全面推进网络安全能力建设，带动网络安全产业发展。

（三）新兴产业蓬勃发展驱动安全创新变革

一是新技术新业态不断涌现，伴生新的安全风险和挑战。伴随新一代信息通信技术在更广范围、更深层次、更高水平与实体经济融合，网络安全风险和挑战也不断渗透、扩散、放大，亟需在工业互联网、区块链、5G、IPv6 等领域加大安全研究力度，提早谋划，预先布局，有效防范不断变化的安全风险。**二是**新兴技术与网络安全融合创新，驱动安全防御能力演进升级。例如，区块链技术推动数据存储方式转型和信任机制重塑，目前已应用于无密钥的签名方案、强认证的安全数据存储等安全场景中。人工智能技术能够更快、更精准、更全面的进行采集和分析，提高攻击威胁等的监测、识别、响应效率，目前已在入侵检测、恶意软件分类、用户行为分析、攻击智能感知等方面取得积极进展。**三是**新兴技术的恶意利用和滥用，倒逼安全防护能力提升。人工智能技术助力网络攻击自动化、智能化，催生新型网络犯罪模式和行为，并将危害影响从网络空间传导至现实社会。面对更为严峻的攻防对抗形势，安全防护理念、思路和技术实现路径也需动态调整、适配。

（四）大型央企战略布局或将重塑产业格局

2015 年以来，大型央企强势进入网络安全领域。中国电子科技集团公司（CETC）集合旗下三十所、三十三所、中电科技公司等单位成立中国电子科技网络信息安全有限公司（简称“中国网安”），近期增持成为绿盟科技第一大股东；中国电子信息产业集团（CEC）战略入股奇安信。从战略布局的驱动因素看，一是源于网络安全上升为国家战略，产业发展前景向好，符合其业绩增长需求；二是源于补齐产业链条，提供覆盖全流程全方位的综合安全能力；三是推进混合所有制改革，放大国有资本功能。通过战略布局，能够更好发挥产业和研发优势，技术互补、资源共享，促进网络安全在信息产业全链条的渗透融合，带动产业技术创新，加速集群式发展。大型央企在成为国家网络安全产业的中流砥柱的同时，也将深刻改变产业竞争格局，引发新一轮角逐。

（五）安全标准体系建设推进安全能力协同

网络安全威胁信息共享和应急处置联动是保障网络空间安全的重要基础。目前，一些重大网络工程、重大科技项目建设往往由不同的主体承担，系统架构、实施路径等存在较大差异，系统间缺乏统一接口，数据资源难以高效、安全对接共享，处置措施难以精准、可靠下达，成为网络安全能力建设的重要制约。打破数据孤岛、增进手段联动需求日益迫切。将关键技术转换为标准，发挥标准的规范、引领作用成为破解建设分散、投入重复、资源壁垒的新思路。工业和信息化部在持续开展网络安全技术应用试点示范工作基础上，正在推动将

优秀项目转化为标准指南，并在行业内推广实践。公安部以自身为切入点，于 2018 年成立全国公安大数据工作领导小组，推进数据融合共享，打造智慧公安“大脑”，并在实践中总结形成操作规范，将产业应用与标准有机结合、紧密互动。

（六）职业技能培训竞赛助力人才队伍建设

网络空间的竞争，归根结底是人才竞争。目前，我国网络安全人才短缺形势依然严峻，从业人员在知识储备、技能等方面尚存短板，网络安全人才队伍建设任务迫切。借鉴国际经验，立足我国实际，网络安全人才队伍建设需要实现三个方面的结合，**一是**将网络安全知识学习与技能实践相结合，通过攻防竞赛等形式，在实践中检验理论学习成果，提升应变能力、实战技能；**二是**将网络安全人才的能力建设与实际场景需求相结合，立足网络安全保障的不同场景和需求，定制针对性培养计划，优化课程体系设置和评价机制，着力加强面向关键信息基础设施领域和工业互联网、车联网等融合领域复合型人才培养；**三是**将网络安全人员能力和岗位职级评定相结合，建立网络安全职位体系，引导形成对岗位职责、发展路径的清晰认知，为人才考核选拔、奖励提升等提供参考。

附件一

我国企业工业互联网安全相关实践

（一）三六零：360 工业互联网安全大脑系统实践

360 工业互联网安全“安全大脑”系统，通过感知、决策、响应三个手段形成一套智能安全系统来应对安全威胁。

建立全天候多维度感知系统。横向感知，通过 ICS 全网资产扫描，全面探测工控企业内网资产暴露在互联网的资产所存在的漏洞，感知内外网攻击横向渗透行为。纵向感知，从 IT 系统到 OT 系统总线感知，监测由于信息安全导致的生产安全问题。交叉感知，内网数据与外网情报交叉分析可快速溯源，定位威胁。工业互联网安全大脑如图附 1 所示。

图附 1　工业互联网安全大脑

基于数据分析及算法建立安全引擎。通过感知获取数据，并对网络行为和数据进行记录，360 拥有全球海量的安全大数据及安全检测规则。以此为基础，利用深度检测、智能分析和安全专家，对大数据进行分析、挖掘和关联，从而快速发现高级威胁。同时通过人工智能算法结合外围威胁情报，安全编排等技术组成工业互联网安全引擎。

形成“一体两翼”安全响应。360 工业互联网安全大脑以打造安全生态模式和大多数工业信息安全厂商进行深度合作，实现“360 工业互联网安全大脑形成决策——>下发策略更新到工业信息安全设备——>实现实时数据上报和动态策略部署——>阻断攻击行为并反馈”。同时 360 设立应急响应中心及安全服务团队，为工业互联网突发事件形成一体两翼的响应体系。

（二）上海观安：基于设备行为分析的网络态势感知系统实践

基于设备行为分析的电力监控网络态势感知系统能够对电力系统各种通信协议、流量信息，电力报文进行深度解析，对电力设备行为进行全面分析，平台在技术架构上采用“采集终端+大数据平台”的分布式部署方式，采集终端以旁路部署在电力网络的各区域和交换机侧，通过交换机镜像口获取网络流量，通过网络发送至大数据监控平台；大数据监控平台接收来自采集终端的报文，进行设备行为分析，主动感知安全威胁，并且对智能电力系统面临的风险进行量化分析，以可视化方式把分析结果展现给电力监控人员进行及时应对处理，确保电力网络的安全运行。关键技术包括：

- 基于设备行为分析的异常检测方法

基于设备行为分析的异常检测方法基于深度解析引擎对数据包进行解析处理，把解析后的数据发送到基线学习模块处理产生设备行为基线；后续来自解码的设备行为数据与自学习模块的设备行为基线进行比对分析，发现其中是否存在不符合通信关系基线的通信行为及非法的新增资产，对异常通信或者异常资产进行告警。能够实时检测针对电力网络的攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒的传播等。

- 电力网络二次设备指纹学习及分层拓扑动态识别

通过分析不同电力报文的特性，对设备进行特征值分析提取，分别通过监督式的分类算法和无监督式的聚类算法对电力网络中各电力设备的拓扑进行识别，用“分类指导聚类，聚类验证分类”的思想进行优化迭代，最终可以做到电力网络动态拓扑的识别。在平台上可以提示用户对新接入设备进行确认，规避非法设备的接入风险。

- 基于事件特征匹配的设备间流量异常检测方法

基于电力报文的特性，在流量异常检测模型中引入各种特征，通过分析特征值，形成异常流量检测模型，用于后续的流量异常检测。

- 电力设备间异常指令检测方法

电力设备间指令异常检测场景包括：（1）设备间高风险指令；（2）设备间异常指令异常。通过引入规则引擎，可以实时检测电力网络中的高风险指令操作，给出告警提示，用户可以进行相应的规则增减。根据采集到电力网络流量，用机器学习模型来进行设备异常指令的检测，触发异常指令告警事件。对于异常指令事件，通过大数据展示平台向用户展示异常结果，提醒用户排查原因，避免后续风险发生。

（三）中国网安：基于工控信息安全管理服务的实践

项目以工控安全管理服务模式，整体化平台化服务保障的方式支撑落实工控安全管理职责，通过对地区工业信息安全管理需求的深入分析，涵盖地区工业控制信息安全管理工作全生命周期，以安全管理服务平台为基础，融合安全服务工具、安全服务团队、培训演练环境、系列服务管理流程和相关政策制度标准为一

体的，全面支撑指导、监测、通报、处置、响应的一体化监管体系及软硬件结合的整体保障服务。

1. 安全服务体系

项目服务体系架构按照 ITSM 理念，参照 ITIL/ITSS 等国际国内标准，实现安全服务过程中“服务工具”、“服务团队”和“服务流程”的有机整合。

2. 服务平台

服务平台对联网工业控制系统主动感知、及时预警，对重点区域、重点行业相关工控系统和设备重点监测，对相关信息开展综合分析和可视化呈现。同时，根据制定的预警策略将感知到的安全威胁和安全事件等进行预警通报和应急响应。平台对收集到的数据进行集中存储，对数据进行脱敏脱密处理后根据要求开放给用户指定的其他分析平台。工业控制信息安全“全域采集、多源汇总、分析研判、风险感知、态势呈现、预警通报、应急响应和相关安全服务管理”为一体的监测服务平台，全面实现工业控制系统信息安全“自动化监测发现、流程化事件处置、任务化预警通报和规范化安全监管”，为工业控制系统信息安全管理服务提供信息化、流程化、规范化和体系化的服务保障。工业控制系统信息安全服务平台整体架构如图附 2 所示。

图附 2 工业控制系统信息安全服务平台整体架构

3. 安全服务

项目主要服务内容包括态势感知服务、在线监测服务、安全检查服务、应急响应服务和安全咨询服务等六大类服务。

（四）天地和兴：集控模式下风电工控安全集中感知平台实践

针对集控模式下风电工控安全的实际问题，通过风场安全防护、汇总关联分析、中心集中展示的方式实现风电工控安全动态防御。

1. 分布式技术架构，周到防护、全面采集、态势展示

平台整体采用三层分布式技术架构，由数据采集层、汇聚处理层和分析展示层组成

- 分析展示层

功能定位：工控安全态势展示。作为支撑开展工控安全监督、考核、管理等工作业务的窗口和抓手，实现工控安全的合规监管和客观量化考核管理。集中保存全网网络安全监测信息，通过机器学习和关联分析完成各业务板块网络安全态势可视化展示。第一级视图：整体安全态势展示；第二级视图：基于物理位置的网络防护拓扑结构展示；第三级视图：下属电厂详细风险信息展示。

- 汇聚处理层

功能定位：平台数据采集的前置终端。集中收集数据采集层获取的生产控制区工控网络异常行为和事件、工控网络违规内外联、工控网络威胁事件、工控主机异常操作和违规 U 盘操作等工控网络安全信息，并完成所采集安全监测数据信息的归一、整形、压缩和转发等数据预处理功能。

- 数据采集层

功能定位：工控安全数据信息采集。一是计算环境数据采集，包括非法程序启动监测、主机非法内外联监测、违规 U 盘操作等；二是网络通信数据采集，包括设备资产发现、设备运行状态监测；三是区域边界数据采集，包括安全合规监测、异常攻击监测、非法外联监测、非法内联监测、内网异常访问监测、非法 Web 服务监测等数据信息。

2. 动态化体系支撑，牢固基础、强化应对、落地运营

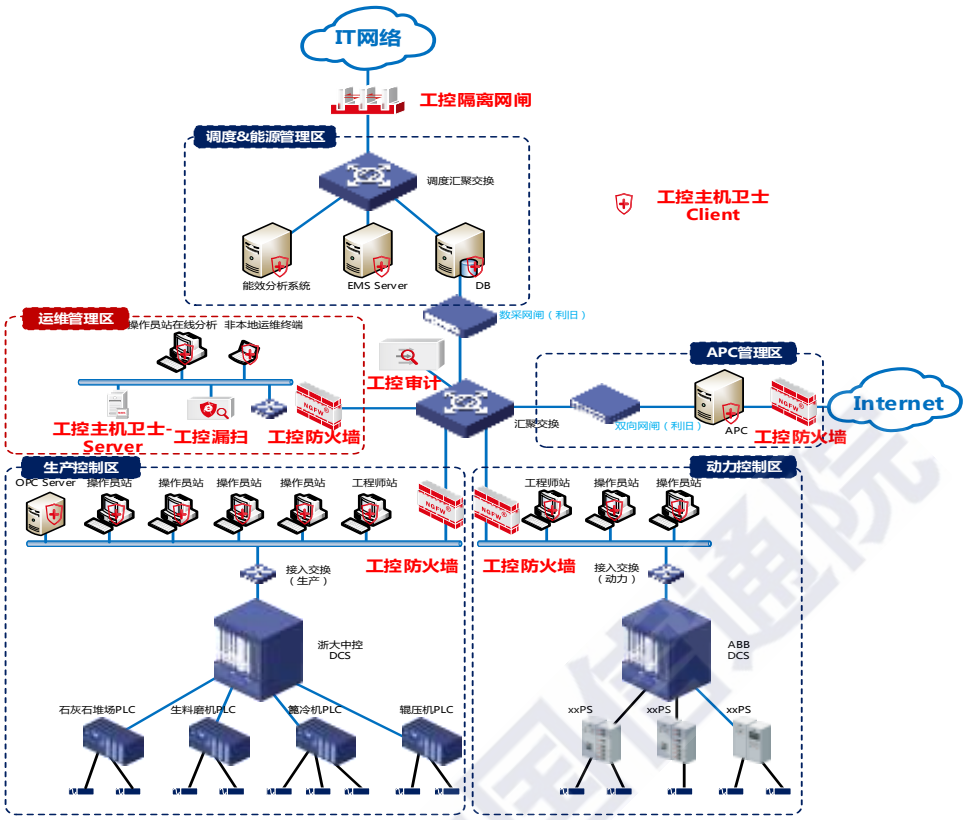
本项目在风电集控基础上应用了基于工业控制系统的防护手段，构建了安全可控为目标、监控审计为特征的风电厂控制系统新一代主动防御体系，提高工业控制系统在于工业互联网对接过程中的整体安全性。项目的成功实施，为发电企业工业控制系统网络安全防护体系建设开创行之有效的安全建设模式，提高发电厂一体化安全防护的能力。平台功能体系如图附 3 所示。

图附 3 平台功能体系

平台结合生产控制系统实际设计，整体具有集中监测控制的特点，底层为各风场机组设备层，上层为区域监控层，分监测模块、审计模块、运维管理模块、主机防护模块、集中管控模块、预警模块等多个功能模块，在现场实现全方位的纵深防御及基础数据采集，在体系架构及运营管理的支撑运行下，达到多级联动、态势分析的效果。

（五）天融信：基于行为基线分析的安全技术防护体系

天融信基于行为基线分析的安全技术防护体系涵盖了安全防护设备、检测设备等体系化的安全产品，解决生产网络信息系统安全问题。整体安全防护部署拓扑图如图附 4 所示。



图附 4 整体安全防护部署拓扑图

- 访问控制

在 IT 至 OT 网络间部署工业网闸，实现网络边界访问控制，满足等保 2.0 中控制区与非控制区边界实现单项隔离即协议剥离要求。

在生产网 OT 网络区域边界部署访问控制手段，对接入访问行为进行管控。同时通过基于用户端的认证手段，实现接入目标的认证。关键节点采用工业防火墙+VPN 的应用方式，实现通信数据保密性和完整性防护。

- 网络行为监测

基于网络行为监测考虑，在应用层面设置监测审计节点，作为流量回溯分析及网络白名单应用。

网络行为监测可监测网络中非授权接入行为，实现工业流量解析，还原对控制器及上位机的访问行为，同时可针对通讯流量进行监测并统计，可将分析记录结果通报大数据分析系统等进行报警、展示。

监测审计网络白名单功能通过自学习或策略设定方式，对网络监测节点协议进行白名单过滤，限定可流通协议，对于限定外协议进行报警，有效保障了控制系统内流量最小化原则，减少非必要带宽占用。

- 工控主机卫士

工控主机卫士客户端部署于生产网全部 PC，通过对终端的管控，构成工业

安全实质层面最外层的安全防线。工控主机卫士 Server 部署于 IDMZ 区域，作为对客户端管控、审计记录的统一监控及策略统一下发。

工控主机卫士以最小化设定为原则，对主机中应用进行管控，对移动存储分级授权。针对目标应用必要进程及服务开放白名单，非限定进程及服务均禁止运行。该策略在保证生产持续进行条件下有效降低对工控计算资源的占用。

- 脆弱性检测

工控漏洞作为一项重要脆弱性指标需有相应的安全防护措施进行应对，建议采用离线工控系统漏洞扫描和入网检测方式进行工控系统脆弱性检测。脆弱性检测对目标设备进行扫描，可发现生产系统中存在的工控漏洞等脆弱性。同时可对生产网中新增设备/系统进行上线前检测，检测合格后方能具备入网资格。

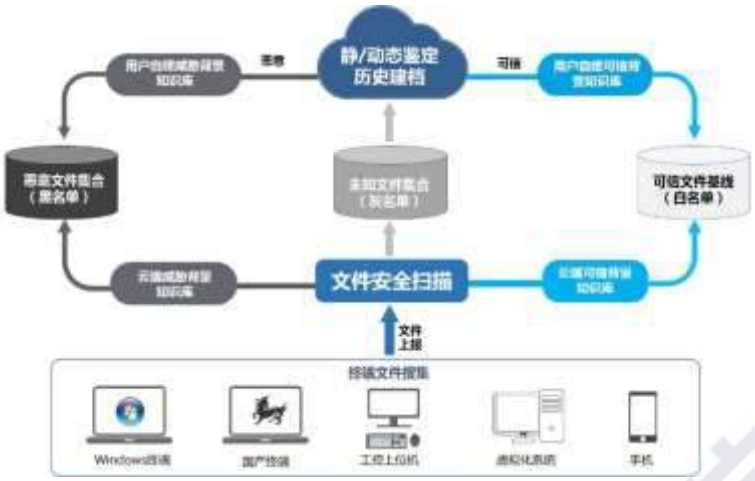
（六）安天：智甲终端防御系统的工业部署实践

安天智甲终端防御系统（简称“智甲”）是专为各行业的业务网络、办公网络、专用网络、桌面虚拟化办公网络、数据中心以研发的终端安全防御产品。

安天智甲终端防御系统以私有查杀云技术为基石，以黑白双控检测为机制，以可信应用控制和主机安全策略为主线，以静态鉴定、程序动态安全分析为手段，以多维度多机制终端安全防护为目的，实现对 APT 高级攻击、勒索软件攻击的全面防护，实现对终端的有效防护。

安天智甲终端防御系统由云平台系统（管理中心）与终端代理软件（客户端）两部分构成。管理中心采用 B/S 管理架构，管理员可以在网内任意一台计算机上通过 Web 方式随时随地登录管理中心实现全网终端安全态势管控。管理中心具有定制和分发系统安全策略、对客户端提交的文件进行安全鉴定响应、收集主机安全日志、漏洞统一管理、管理员权限分配等功能。

安天智甲终端防御系统主要包括以下功能：系统管理、威胁展示、可视化展现、病毒查杀、漏洞检测与修复、主动防御、高级威胁防护、APT 追溯、虚拟补丁防护、防勒索、终端管理、检测加固、网络保护、安全基线、移动介质管控、流量控制、威胁报表、日志与审计等功能。安天智甲终端防御系统如图附 5 所示。



图附 5 安天智甲终端防御系统

- 终端管理

可查看网内终端信息，包括：计算机名、IP 地址、MAC 地址、CUP 占用率、内存容量、TCP 连接数、硬盘容量、客户端版本、操作系统、数据库、应用软件版本等信息。可管控配置客户端防护策略，包括：客户端启动策略、升级策略、防护策略、上传策略、扫描策略等。可进行终端安全状态评估，对全局终端安全性进行监控。评估终端安全状态，可查看终端威胁文件、未知文件、未知文件执行、系统高危漏洞、终端安全状态等信息。支持分组管理，可对不同组下终端配置不同防护策略。

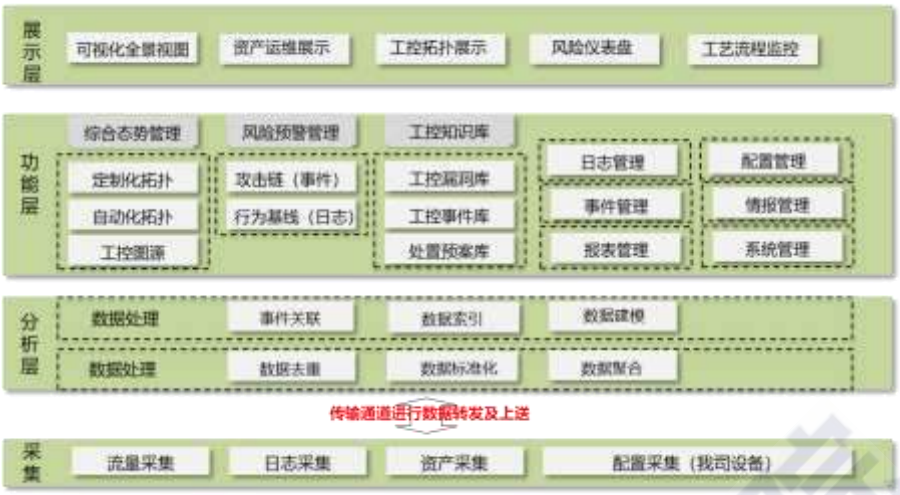
- 威胁展示

展示全局安全状态信息，包括病毒事件统计信息、高级威胁统计信息、系统高危漏洞统计信息；以未知文件统计信息、文件云鉴定统计信息、威胁可视化等。还有系统通知信息，安全基线，威胁终端排名。显示当前分级以及当前分级以下分级的威胁统计信息，以分级为统计对象，显示各级的病毒、漏洞统计信息以及文件鉴定建议统计信息。

（七）绿盟：工业网络安全智能监控预警平台实践

绿盟工业网络安全监测预警平台从工业控制系统安全的角度，对工控系统的各类 IT 和 OT 设备数据进行采集，包括业务设备日志采集、安全设备事件收集、网络流量数据采集、安全设备配置采集等功能。平台对采集得到的结果进行统一分析与展示，发现工控网络内部的异常行为，如新增资产、时间异常、新增关系、负载变更、异常访问等行为，实现对工控现场安全事件的预警与响应。

绿盟工业网络安全监测预警平台可以对工业网络中各类上位机服务器、工控终端、网络交换设备、工控安全设备进行集中化的性能状态监控、安全事件的集中展示、安全风险的评估、工控分区分域的健康等级，以及依赖于工控知识库的安全响应与处置。绿盟工业网络安全监测预警平台如图附 6 所示。



图附 6 绿盟工业网络安全监测预警平台

- 工业网络数据采集

绿盟工控预警平台可以支持代理日志采集方式和多种标准协议。通过数据采集、数据理解、数据抽取和数据清洗等操作，将各种应用系统和设备的日志进行预处理，帮助管理员把工业网络日志进行去噪，提取其中人们事先不知道，但有潜在有用的信息和知识。

- 独家数据强化技术

绿盟工控预警平台根据绿盟科技对攻防研究的长期积累，提供一套简洁有效的日志统一分类，使用独有的技术将日志快速标准化，并基于安全分析需要进行数据的过滤和强化，丢弃无法用的噪音信息，提升日志查询和分析效率。

- 强大的分析引擎

平台中预制关联分析引擎，预制引擎构成分析平台的核心功能并且对专项分析提供基础能力，如风险分析、脆弱性分析、态势分析、资产分析、攻击链条分析等。

分析引擎采用分布式设计能够进行横向扩展，面临工业网络数据量时能够实现按需扩展，将分析引擎分散到其他更多的机器中，实现按需进行计算资源扩展。

- 面向业务的插件化设计

绿盟工控预警平台采用全新大数据框架，将上层业务模块插件化处理，使业务模块与平台功能进行一对一设计，业务模块的改善和增加就不会造成其他模块或平台功能的调整，也就是将业务模块抽象并与平台功能实现分离，从而提高研发效率，降低企业维护成本。

- 可靠性

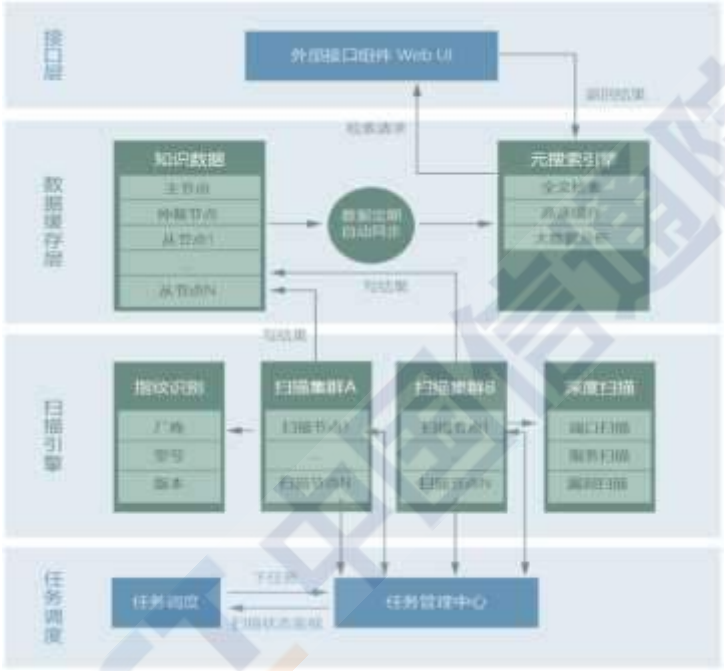
绿盟工控预警平台采用大数据组件，对数据对象弹性分布存储 3 个存储节点中，并采用线程级监控，一旦发现问题，可迅速恢复并告警，同时 3 备份可以提供完整的灾难恢复功能。

- 多地部署

针对大型多组织的企业和机构，采集器可以部署在异地站点或二级单位（保持网络可达），分析中心部署在总部节点，异地站点将采集到的数据定时通过 FTP 或 SFTP 上传到上级分析中心，供本地留存和查询服务。

（八）威努特：基于无损探测的工业互联网设备测绘实践

威努特自主研发的工业互联网雷达 iRadar 旨在发现暴露在互联网上的工业设备、工业系统、物联网设备等。工业互联网雷达产品架构图如图附 7 所示。



图附 7 工业互联网雷达产品架构图

- IoT 设备扫描

工业互联网雷达 iRadar 采用分布式并行扫描技术，扫描节点动态可扩展，实现了网络空间设备快速扫描。工业互联网雷达采用了流水线作业式探测技术，来提高探测效率。设备探测过程包括端口存活、服务判别、设备识别、漏洞发现等多个步骤，每个步骤作为流水线的一个环节，实现了细粒度的扫描任务调度。工业互联网雷达引入了无状态极速扫描技术，使用了 TCP 半连接扫描和异步状态统计的相结合的模式，大幅度的提升了单次扫描的速度。

- 基于指纹的设备类型识别

工业互联网雷达引入了多维度的协议识别技术实现了广泛的协议解析。此外，平台采用会话深度交互技术，可获取工控设备固件的型号、版本等多种信息。

工业互联网雷达除可识别 HTTP、HTTPS、FTP、Telnet、SNMP 等通用协议外，还支持主流工控协议识别，如 Modbus、S7、DNP3、IEC104 等，覆盖西门子、施耐德、罗克韦尔等国内外知名厂商的 PLC、DCS、RTU、SCADA、HMI 等

工控系统。

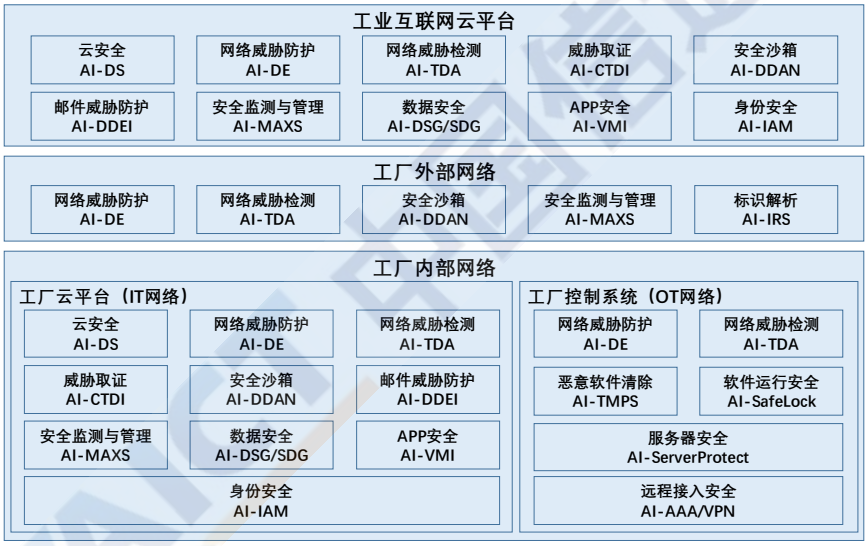
- 基于业务报文的无损漏洞探测

对于工控系统等重要信息基础设施，业务的连续性与稳定性是至关重要的。传统的有损漏洞探测方式并不适用此类设备。传统的扫描产品为了保证漏洞识别的精准度，探测器会向被探测设备发送含有一定攻击特征的报文，会对目标系统带来攻击性和不稳定性。

工业互联网雷达采用无损漏洞探测技术，利用正常协议控制命令，获取设备漏洞信息，保证探测行为与业务行为的一致，从而实现了在不影响系统正常作业基础上的漏洞探测。

（九）亚信安全：工业互联网安全解决方案及应用实践

针对工业互联网的安全需求，基于亚信安全目前成熟的解决方案，将工业互联网划分为工业互联网云平台、工厂外部网络和工厂内部网络来提供安全能力架构。安全能力架构如图附 8 所示。



图附 8 安全能力架构

- 针对工业互联网云平台提供了工业云平台安全、工业网络威胁检测、工业网络威胁防护、威胁取证、安全沙箱、邮件威胁防护、安全监测与管理、工业数据安全、工业移动终端及 APP 安全、身份管理安全等能力；
- 针对工厂外部网络提供了协议标识解析、网络威胁检测、网络威胁防护、安全监测与管理等能力；
- 针对工厂内部 OT 网络提供了工厂控制系统网络威胁检测、网络威胁防护、恶意软件清除、软件运行安全能力；针对工厂内部 IT 网络提供了云平台、主机安全、数据安全、邮件威胁防护、安全沙箱、身份安全、安全监测与管理等能力。

在汽车制造业中提供了以精密联动为核心的 APT 防护系统解决方案，作为

未知威胁信息采集（邮件网关 IMSA、DDEI）、网关（下一代安全网关 Deep Edge）及终端处理节点（TMCM\OSCE），并新增未知威胁分析、网络传输已知威胁检测及未知威胁采集（TDA）、网络防毒墙阻断新威胁 IP/URL/文件/漏洞利用（DE），形成威胁源头捕获、威胁分析、威胁处理的一个完善流程，通过联动方式自动完成，将 APT 威胁得到有效及时的处理。

（十）启明星辰：基于流量自学习的工业互联网设备深度网络逻辑隔离安全防护实践

天清汉马工业防火墙可部署在工业网络每层的边界位置，或部署设备层的边界对不同的工厂进行逻辑隔离。

1. 工业协议访问控制

工业防火墙可以对专用的工业协议进行白名单或黑名单的访问控制：

- 预置了百种以上工业协议，可实现工业协议的白名单安全防护；
- 预置了常用的 PLC 防护模型，可快速实现控制器的白名单防护；
- 支持基于二层协议号和三层网络端口号的自定义工业协议白名单安全防护。

2. 工业协议深度过滤

天清汉马工业防火墙针对工业协议的安全防护，除了具备白名单访问控制等基本功能外，还需要对工业协议有应用层的理解与控制，可以实现对工业指令的过滤。天清汉马工业防火墙支持基于 Modbus/TCP、Modbus/RTU、IEC104 等协议的深度过滤功能。以下以 Modbus/TCP 和 Modbus/RTU 为例进行说明：

- MODBUS/TCP 深度解析防护

天清汉马工业防火墙的 Modbus/TCP 深度解析模块可以支持应用层细粒度控制，具体包括：功能码的访问控制、设备地址的访问控制、线圈范围的读写访问控制、寄存器范围的读写访问控制、输入地址访问控制等。此外还通过支持阻断时 Reset 回复、阻断时异常回复和黑白名单机制来保证工业网络在防护设备阻断时不会出现异常。

管理员通过对业务和实际生产网络的梳理，可以建立起合法业务的 Modbus 指令列表，通过 Modbus 深度解析防护模块可以建立合法白名单，阻止非法和入侵的报文通过，极大提高 Modbus 网络的安全防护能力。

- MODBUS/RTU 深度解析防护

虽然工业以太网是发展趋势，但很多生产线仍是基于串行链路进行通信。天清汉马工业防火墙支持基于 RS232/440/485 链路的数据通信，同时可以支持引用 Modbus/RTU 的深度解析防护策略。

天清汉马工业防火墙支持串行通信参数配置，可以针对波特率、数据位、奇偶校验、停止位、流控参数进行配置。

3. 工业入侵防御

天清汉马工业防火墙集成特有工业入侵防御引擎，可以对工业系统的私有协议或者特定攻击进行防护。其引擎独创的规则定义语言支持 TCP、UDP、HTTP、DNS 等 60 多种协议解析；支持 300 多种协议变量的解析，且协议变量名称遵循国际标准；提供百余种功能函数专用于规则描述，简化复杂规则功能的定义；支持 24 种算术运算符、逻辑运算符和多种数据类型。可以精确表达类似自然语言的丰富的检测需求，减少误报的同时可增强发现各种多样化、复杂化、隐蔽化的攻击。

4. 流量自学习

为了解决现场工程师熟悉业务但对工控网络协议不太了解的情况，设备支持在添加防护策略前，在工控环境中进行流量自学习。

设备首先通过自学习获取工控设备的 IP、MAC 地址、工业协议等信息；然后对工控设备进行自动命名，以资产和协议的角度更加形象化地梳理并呈现工控网络情况，并进行向导式的安全策略推荐。

5. 多工作模式

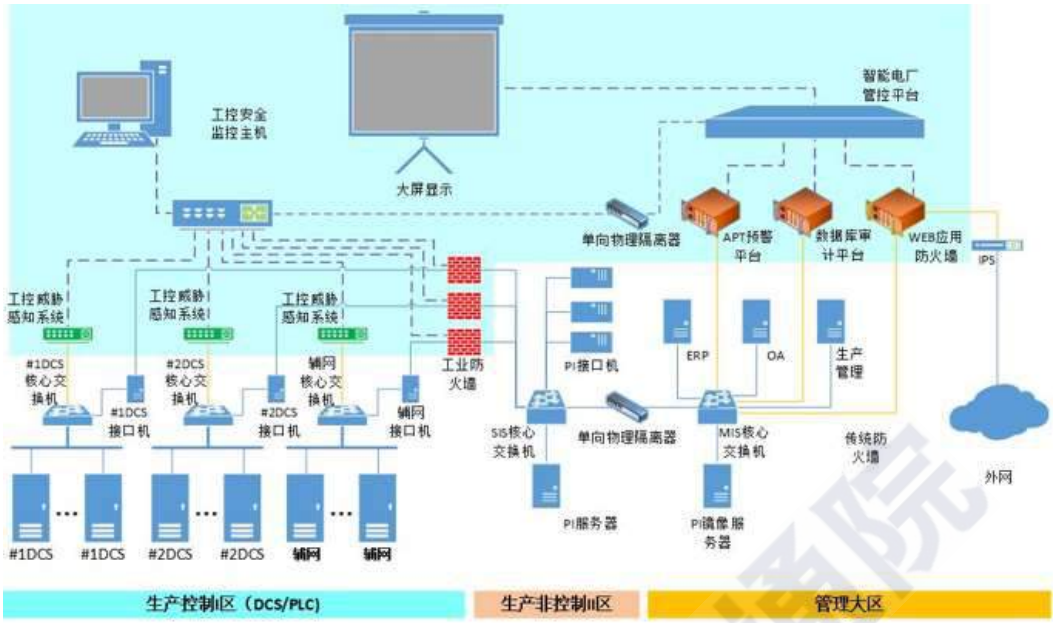
工业网络对可用性要求最高，管理员需要完全掌握工业网络的运行情况后，才能根据实际情况制定合适和有效的安全策略。天清汉马工业防火墙支持三种工作模式，分别是：

- 全通模式：所有报文都通过，保障网络畅通。
- 测试模式：针对要阻断的报文并不实际丢弃，而是以日志报警的方式告知管理员，主要用于管理员理解策略的效果是否符合预期。
- 防护模式：安全策略经过测试模式的考验，管理员对效果进行了充分的评估，并将策略调整到最优，此时可以切换到防护模式，对工业网络进行安全防护。

（十一）安恒信息：发电厂电力监控系统信息安全防护实践

电厂工控网络和信息安全防护体系建设是根据“纵深防御”安全原则。不仅加固管理大区信息安全防护手段，同时通过对工业控制系统进行安全区域划分，建立不同区域之间的数据通讯管道，对管道数据进行全面的分析与管控。中央管理与控制平台必须使企业管理者能够总揽全局，时刻了解工业控制系统网络安全的状况，指导企业建立合理的安全策略，规范安全管理流程，建立工业控制系统网络安全的“纵深防御”体系。

在本电厂中建立“纵深防御”体系如图附 9 所示。



图附 9 工控及信息系统智能防护解决方案网络图

1. 加固管理大区信息安全防护

在信息大区部署安全防护产品，对 Web 攻击及 APT 攻击进行过滤和预警，具体措施如下：

- 在四区核心交换机上采用旁路接入的方式部署数据库安全审计系统；
- 在四区核心交换机上采用旁路接入的方式部署 APT 攻击预警平台；
- 在四区在 IPS 与防火墙之间部署 Web 应用防火墙。

2. 实现生产大区工控安全防护

在生产大区部署工控安全防护产品，提高工控系统在边界隔离、入侵检测及安全审计等方面的防护能力，具体措施如下：

- 在 1 号 DCS 根交换机上采用旁路接入的方式部署工控威胁感知系统；
- 在 2 号 DCS 根交换机上采用旁路接入的方式部署工控威胁感知系统；
- 在辅网核心交换机交换机上采用旁路接入的方式部署工控威胁感知系统；
- 在 1 号机 DCS OPC Server 与 PI 接口机之间部署工业防火墙；
- 在工业废水处理 PLC 与水网核心交换机之间部署工业防火墙；

3. 实现全厂安全信息运营

在四区部署企业安全感知中心，收集部署在生产大区及管理大区安全设备提供的安全数据，其中生产区的安全数据通过单向隔离装置导出，保障生产大区的物理隔离。

企业安全感知中心为本方案中的工业控制系统信息安全的中央管理与控制平台，实现对工业控制系统及设备、安全设备等的监控。

（十二）杭州迪普：智能工业交换机助力工业互联网高可靠通讯的实践

迪普科技基于白名单分析的安全通讯体系包含了智能工业交换机、物联网应用安全控制系统等产品，是为满足灵活多变的工业应用需求而提供的一种工业以太网通讯解决方案，解决用户网络的环境适应性、通信实时性、网络安全性等问题。

- 适应恶劣环境

智能工业交换机严格遵守工业规范要求而开发，整机采用工业级元器件，无风扇散热电路设计，经过严苛的环境测试，设备能够在-40~85℃宽温环境下稳定工作。提供了耐振动 、耐冲击、耐高/低温、耐腐蚀、防尘、脉冲磁场抗扰等卓越的工业级品质，确保在各类恶劣环境下可持续可靠运行。

- 整机掉电告警机制

智能工业交换机的整机掉电告警机制，使网络运维人员可实时通过网管界面有效了解工业交换机的供电状态。当设备运行过程中出现掉电，交换机将用其内部的储能电路向网管界面及时发送掉电告警提示信息，使工作人员能远程了解交换机的供电状况，及时做出相应的处理。有效缩短故障恢复时间、节省运维成本、提高资产在线率。

- 视频数据探测安全防护技术

智能工业交换机使用视频数据探测安全防护技术，可实现不同厂商的摄像头接入到交换机时，交换机能够自动识别摄像机厂商的型号以及 TCP 端口、摄像机 IP、MAC 等信息，对正确识别到的摄像机信息进行端口数据绑定操作，只放通绑定的摄像头流量，保证数据正常转发，当非绑定设备接入交换机时，会对其接入端口进行隔离，防止黑客通过 PC 进入视频传输网进行一系列违规操作，对网络进行安全防护。

- 白名单防护机制

智能工业交换机可与物联网应用安全控制系统 DAC 进行联动，信息监控平台将两者收集到的接入终端信息形成资产库白名单，配合 DAC 设备内置的协议白名单，实时识别非法设备及非法业务流量，并将日志发送到信息监控平台，平台将通知交换机，交换机可溯源到终端接入端口并对其进行阻断，将安全防线前移。

（十三）奇安信：工业主机安全防护系统应用实践

面对工业主机补丁打不了、漏洞防不了、资产查不了等安全问题，奇安信集团自主研发了一款面向工控环境专用的工业主机安全防护系统。该系统能够防范恶意程序运行、集中安全风险分析和配置管理，实现对工业主机全面的安全防护。

- 白名单管控

工业主机安全防护系统采用“白名单”防护技术并结合外设管控技术，全方位地保护主机的资源使用。根据白名单策略，工业主机安全防护系统会禁止非法进程的运行，并通过基于单个 ID 的 USB 移动存储外设管控，禁止非法 USB 设备的接入以及合法 USB 设备的权限管控。

- 工业主机“永恒之蓝”防御，关卡式病毒拦截

针对 “永恒之蓝”勒索病毒，白名单在防护模式下会放行正常的操作系统进程及专用工业软件，主动阻断未知程序、木马病毒、恶意软件、攻击脚本等运行，同时结合漏洞防御进行永恒之蓝的超前防御，可以形成从“病毒入口-病毒运行-病毒扩散”三个环节的层层设防，步步拦截，从而做到病毒进不来、启不动、扩散不了，实现主机安全无死角病毒防护。

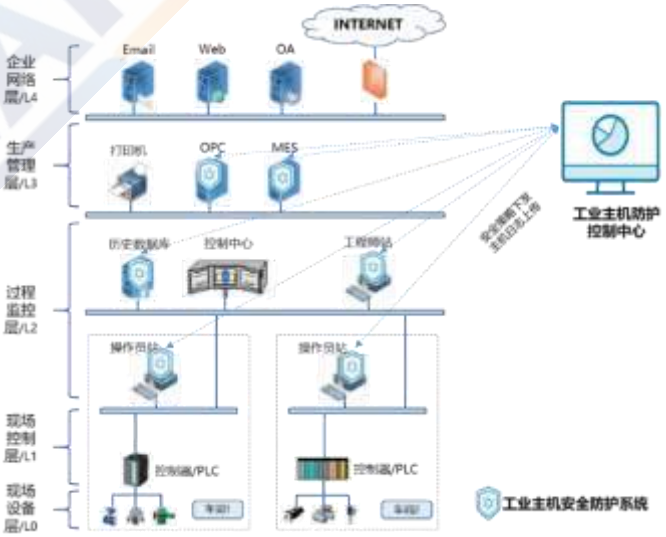
- 工业资产全方位梳理

工业主机安全防护系统通过定义网络 IP 段分组，对指定的网络分组进行周期性地发现并统计网络中的终端数量及类型，自动获取工业主机 CPU、内存、硬盘等基础信息，形成资产清单，为企业进行工业主机管理和安全运维提供有效的参考。

- 集中管理，统一运维

工业主机安全防护系统控制中心采用软件化方式安装在客户的服务器以及虚拟机上，方便系统管理员通过控制中心对网内所有工业主机进行安全策略管理、配置下发等，实现统一管控和安全风险分析，集中管理会显著降低运维成本。

工业主机安全防护系统创新性地采用“漏洞利用分析-流量解析比对-可疑攻击阻断”的超前防御模式，通过白名单智能匹配、“入口-运行-扩散”三重关卡拦截技术及“永恒之蓝”专杀技术，保护工业主机不受病毒等恶意软件侵害。工业主机安全防护系统部署如图附 10 所示



图附 10 工业主机安全防护系统部署

附件二

我国企业云安全相关实践

（一）三六零：360 云安全大脑实践

1. SaaS 云安全能力

三六零云探系统是一款基于 SaaS 的安全服务产品。依靠 360 安全大脑强大的云端资源，以及 360 在搜索、终端安全、Web 安全、云安全等方面积累的数亿用户群和海量数据，为用户提供网站漏洞扫描、网页篡改监测、网页挂马监测、黑词/暗链监测、可用性监测、仿冒/钓鱼网站监测、未知资产监测、DDoS 攻击监测等安全监测服务。三六零云探系统旨在通过云端大数据能力，发现企业网站的安全问题。三六零云探架构如图附 11 所示。

产品设计目标：（1）解决网站未知资产监控问题；（2）解决网站问题发现不全问题；（3）解决网站 0Day 漏洞发现问题；（4）解决网站漏洞修复闭环问题；（5）解决全国可用性监控问题。

产品组成与架构：

- 爬虫引擎是监测平台重要的基础组件，完成对监测域名的内容爬取，以供各类分析引擎使用。
- 大数据平台存储爬取的页面数据，检测的数据等，可用于后续做大数据分析和数据挖掘。
- 内容监测 API 和运维平台主要针对已有数据进行分析,为平台提供监测结果。
- 监测平台 API 和运维平台主要是将群监测的功能界面化,方便用户的日常监控及运维管理。

图附 11 三六零云探架构

三六零云探可以为用户提供快速定位问题资产，提供实时托管式的安全监控

服务，支持本地化和云端的 SaaS 化部署模式，满足各种用户部署要求。

除了三六零云探系统，360 还提供三六零磐云 Web 应用安全防护系统，为用户提供一套基于云+端的，完整的“事前预警+事中防护+事后服务”Web 安全云解决方案。

2. 云安全集中管理平台能力

通过 NFV（网络功能虚拟化）技术把传统网络安全设备进行虚拟化以适应虚拟化云计算环境，打造可以为云上用户动态获取到云安全资源，从而使云上用户可以按需获取相应的安全能力，满足自身业务安全防护、等保合规和安全运营的需求。云安全集中管理平台集成有丰富的安全服务组件能力，包含网络安全、主机安全、应用安全、数据安全以及安全运维审计等安全能力，可以对异构多云平台统一安全管理，安全服务编排、自助安全运营等。

（二）山石网科：基于 NFV 框架的云计算租户级硬件防火墙防护方案

为满足业务迁移上云的安全性，山石网科与某国内知名电信厂商配合，基于 OpenStack 标准框架，实现分行测试云的建设。为实现租户级的安全防护，和租户的自服务。租户之间的安全防护，首先利用 SDN 实现二层网络隔离。租户之间和租户与外部的网络访问控制采用 OpenStack 的标准 FWaaS 实现，由山石网科的硬件下一代防火墙和云集配合 SDN 和云平台完成。山石网科硬件下一代防火墙通过 vSYS 功能（一虚多），为每个云租户创建一个虚拟防火墙，防火墙提供访问控制、NAT 等相关功能。租户的自服务，租户通过在云管平台进行配置、创建防火墙。

山石云·集在方案中扮演 VNFM 和 EMS 的角色。山石云·集提供了标准的 FWaaS 的轻量级插件，用于从云管平台获取配置信息。根据 FWaaS 上生成的创建防火墙、配置防火墙的信息，由山石云·集对硬件防火墙（或虚拟防火墙）进行生命周期的管理，创建防火墙，配置的注入。同时山石云·集也提供了对 SDN 的接口，利用 SDN 接口，对 SDN 进行配置，以确保和 SDN 配置和生命周期的同步。山石云·集会保持所有对防火墙或虚拟防火墙配置的状态信息，以及自身运行状态的信息，一方面方便用户在出现故障时能够及时参与故障排查和恢复，

山石云·集设计时完全参照了 NFV 框架，扮演 NFVM 和 EMS 的角色，并提供标准化 RestAPI 接口。当环境中有 MANO 时，可以配合 MANO、VIM 完成自动化编排部署工作。它向 MANO 提供相关设备信息，便于 MANO 进行编排管理，在 MANO 完成 SDN 配置调整同时，完成防火墙的创建和配置管理。山石云·集可以自动完成网元管理，包括根据网元运行负载进行扩缩。

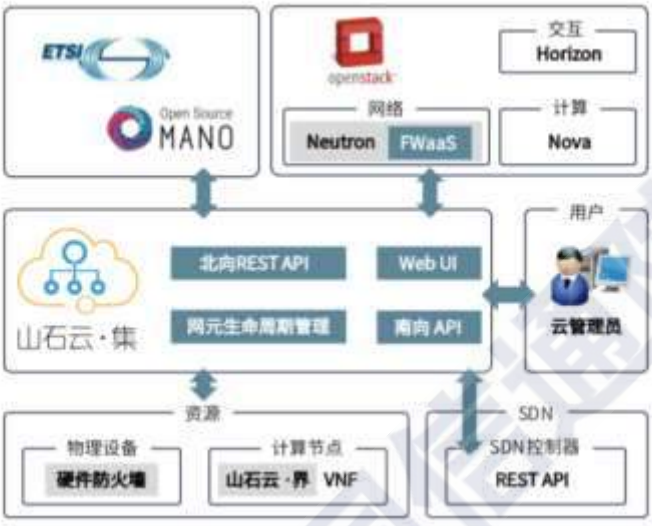
方案的特点是：

- 标准化方案，基于事实标准 OpenStack 框架或 NFV 标准框架，可实现多

个厂家云管平台、SDN 的对接，山石网科已与多个国内厂家完成对接。

- 自动化部署，租户自服务、云、网、安全自动开通。
- 故障可定位、可排障。
- 平滑向全虚拟化方案过渡，方案未来具备向虚拟网元方向发展。

山石云·集 云安全建设方案如图附 12 所示。



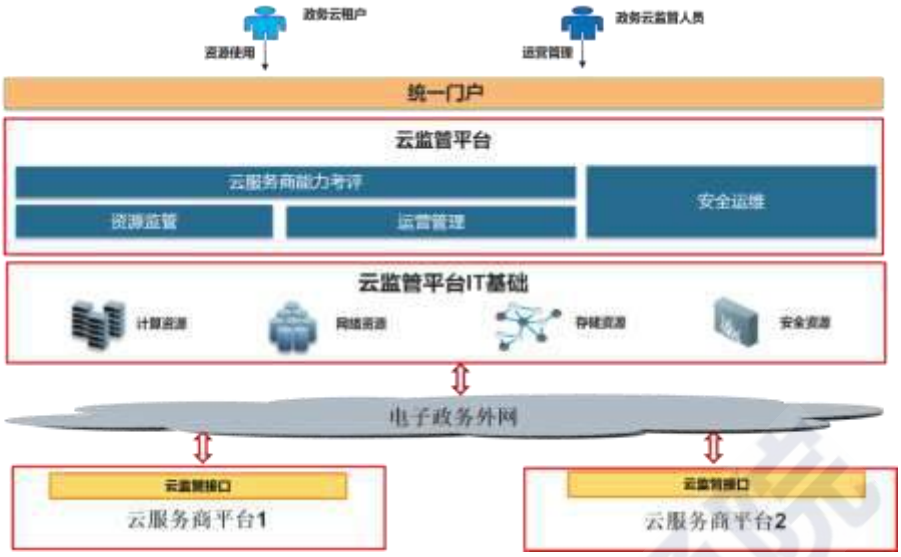
图附 12 山石云·集 云安全建设方案

（三）中国网安：基于第三方的政务云安全监管实践

项目基于第三方监管的理念，针对多级云平台、多种云服务商、多种云平台技术路线的混合云场景，通过统一平台实现资源管理、安全管理与云平台的解耦，为政务云、大型企业等云用户提供对云服务的统一资源监管、统一安全监管、统一运营管理功能，帮助云用户解决混合云场景下的统一监管体系，符合等保 2.0 集中管控、持续监管的思想，是行业内云安全综合管理、Cloud SIEM、混合云管理等的云安全热点问题的落地方案。

1. 基于第三方的多云监管体系

在整体架构中，云监管平台底层通过云资源适配层（接口适配）的标准数据接口接入不同技术路线的多个云服务商平台资源数据、安全数据等，支持异构云服务商，也支持汇聚下级云监管平台采集的数据和分析结果。上述数据汇聚到云监管平台后，通过平台整理、关联、分析、挖掘，对上提供对多个异构云服务商平台的统一资源监管、运营监管、安全运维、云服务商能力考评等功能。上述功能，通过统一门户提供给云租户和云监管人员使用。基于第三方的多云监管架构如图附 13 所示。



图附 13 第三方多云监管架构

2. 云监管能力

云监管平台为云用户提供的主要云监管能力包括资源监管、运营管理、云服务商能力考评和云安全运维。

资源监管主要提供资源运行状态监管、资源变更情况监管、资源配置情况监管、资源故障告警情况监管、资源统计分析报表及租户自身资源操作功能模块，支持全局视角、云服务商视角、租户视角、业务视角及单个资源视角等维度的监管。

运营管理将底层资源包装成标准的可度量的标准化服务对外供应。实现服务目录管理、订单全生命周期管理、用户资源占用的计量和计费、运营情况的报表统计分析等。

云服务商能力考评帮助云监管平台监管人员对云服务商所提供云服务的综合监管，由云服务性价比考评、云服务商运维水平考核及云服务商安全审查功能模块组成。

云安全运维包括态势感知、安全预警、综合运维、应急响应、硬件准入管理、安全审计功能和安全服务支撑模块，对整个政务云平台安全设备进行统一管理，对接入政务云平台的各种硬件设备做准入审批，对政务云平台进行集中安全监管。

（四）天融信：云安全解决方案实践

天融信云安全解决方案，是天融信云安全纵深防御思想的完美体现，采用安全资源池实现租户边界防御，融合基于无代理技术的虚拟化分布式防火墙进行东西向防护，结合 EDR 进行云主机内安全防护，通过云安全管理平台进行统一管理和云安全态势呈现，构成了从外到内多层纵深主动防御体系，全面保障政务云安全。云安全防护产品示意图如图附 14 所示。

图附 14 云安全防护产品示意图

- 统一管控

采用统一云安全管理平台对安全网元集中管控，实现安全服务一键部署、自动激活。用户通过安全管理平台对安全网元进行集中化运维，避免大量安全设备带来的账号管理困难、运维操作复杂等难题。

- 动态可视

通过运维监控大屏页面，对安全资源使用情况、业务系统安全风险进行统一展示，方便运维人员及时发现性能告警、安全威胁。

- 按需购买

安全资源池为租户提供丰富的安全网元，允许租户根据业务发展的安全需求按需购买，满足个性化防护需求，提供差异化安全防护能力。

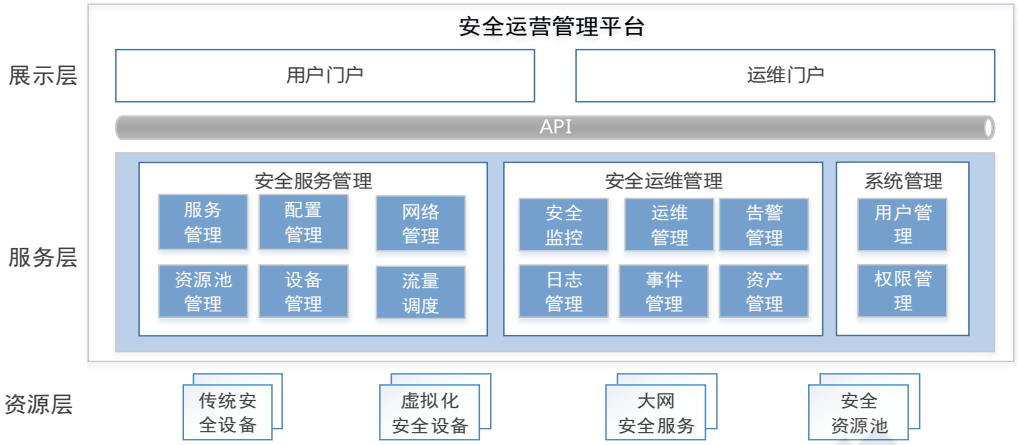
- 深度融合

资源池与上层云平台深度集成，通过云平台账户直接开通、配置资源池中的安全网元，增加使用便捷性。分布式防火墙与云平台深度融合，采用零信任、微分段模型，实现以虚机为单位的东西向安全防护。

（五）绿盟：基于安全资源池的云安全服务平台实践

1. 总体技术实现架构

充分考虑云计算的特点和优势，以及最新安全防护技术发展情况，提供资源弹性、按需分配的安全能力。云平台安全技术实现架构如图附 15 所示。



图附 15 云平台安全技术实现架构

展示层：提供安全服务用户开通、使用、配置各种安全服务的门户，提供安全运维人员对云平台进行统一管理、监控的门户。

服务层：是安全运营服务平台的核心，其负责安全设备管理、安全资源池的管理以及提供用户开通安全防护时所需的流量调度功能。在安全防护设备/服务启用后，还提供服务管理、配置管理、告警管理能力。同时，提供各种安全资源/设备的日志、事件、运维、性能、监控和告警管理。另外，还提供了用户账户、权限等系统管理功能。

资源层：包括了各类安全资源，如传统安全设备、虚拟化安全设备、大网安全防护服务以及专用安全资源池等。这些安全资源接收上层安全管理平台的管理，对外提供安全保障能力。

通过此技术实现架构，可以实现安全服务/能力的按需分配和弹性调度。当然，在进行安全防护措施具体部署时，仍可以采用传统的安全域划分方法，明确安全措施的部署位置、安全策略和要求，做到有效的安全管控。

2. 平台功能框架

安全运营服务平台功能框架如图附 16 所示。

图附 16 安全运营服务平台功能框架

- 安全服务平台

平台用于云环境下的安全服务，可以统一管理云平台中的各种资源。平台基于安全资源池提供的安全能力以服务化的方式提供给管理员，提供管理、控制、分析、呈现功能的组件。

- 安全资源池

支持物理安全设备和虚拟安全设备等类型的安全资源，接受资源池控制器的管理，对外提供相应的安全能力。目前，安全资源池中包含了系统扫描器、Web 应用防火墙、入侵检测系统等安全组件。

- 资源池控制器

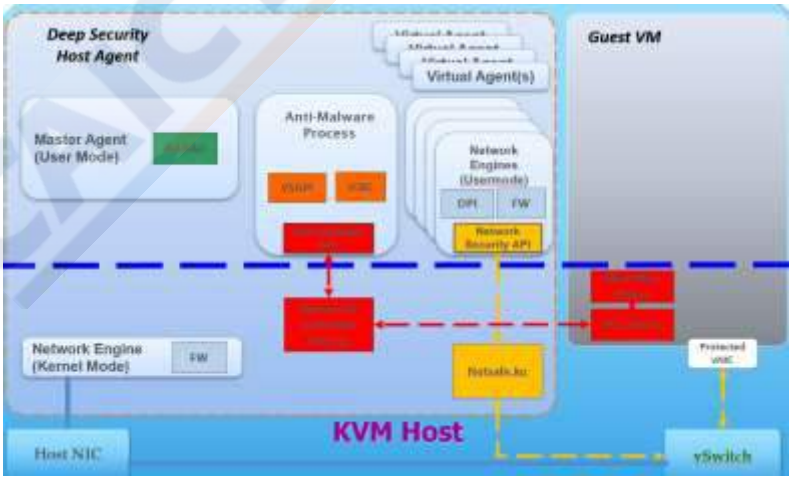
控制硬件和虚拟化的安全设备，提供安全策略管理、配置管理、安全能力管理等与特定安全密切相关的功能。根据应用场景的不同，可灵活配置和扩展。

- 日志分析系统

日志分析系统可以收集设备日志，实现日志的统一管理，将设备用户行为记录下来，便于 IT 运维人员进行快速分析和查询。

（六）亚信安全：服务器深度防护实践

亚信安全针对云化环境提供的信息安全防护方案——DeepSecurity，通过病毒防护、访问控制、入侵检测/入侵防护、虚拟补丁、主机完整性监控、日志审计等功能实现虚拟主机和虚拟系统的全面防护，并满足信息系统合规性审计要求。亚信安全针对虚拟化环境提供创新的方法解决安全防护程序带来的资源消耗问题，通过使用虚拟化层相关的 API 接口实现全面的病毒防护。DeepSecurity 部署如图附 17 所示。



图附 17 DeepSecurity 部署图

亚信安全针对虚拟系统中通过接口实现针对虚拟系统和虚拟主机之间的全面防护，无需在虚拟主机的操作系统中安装 Agent 程序，即虚拟主机系统无代理方式实现实时的防护，这样无需消耗分配给虚拟主机的计算资源和更多的网络资

源消耗，最大化利用计算资源的同时提供全面病毒的实时防护。

- 访问控制

亚信安全 DeepSecurity 防火墙提供全面基于状态检测细粒度的访问控制功能，可以实现针对虚拟交换机基于网口的访问控制和虚拟系统之间的区域逻辑隔离。DeepSecurity 的防火墙同时支持各种泛洪攻击的识别和拦截。

- 恶意代码防范

亚信安全 DeepSecurity 提供全的主机恶意代码防护功能，可以防护传统恶意代码和新型的安全威胁（例如：勒索软件、挖矿病毒等）。并提供机器学习功能，对于同一恶意软件家族的变种。

- 入侵检测/防护

DeepSecurity 除了提供传统 IDS/IPS 系统功能外，还提供虚拟环境中基于政策的（policy-based）监控和分析工具，使 DeepSecurity 更精确的流量监控、分析和访问控制，还能分析网络行为，为虚拟网络提供更高的安全性。

- 虚拟补丁防护

亚信安全 DeepSecurity 通过虚拟补丁技术完全可以解决由于补丁导致的问题，通过在虚拟系统的接口对虚拟主机系统进行评估，并可以自动对每个虚拟主机提供全面的漏洞修补功能，在操作系统在没有安装补丁程序之前，提供针对漏洞攻击的拦截。亚信安全 DeepSecurity 的虚拟补丁功能既不需要停机安装，也不需要进行广泛的应用程序测试。虽然此集成包可以为 IT 人员节省大量时间。虚拟补丁防护如图附 18 所示。

图附 18 虚拟补丁防护

- 完整性审计

亚信安全 DeepSecurity 产品可以针对系统支持依据基线的文件、目录、注册表等关键文件监控和审计功能，当这些关键位置为恶意篡改或攻击时，可以提供为管理员提供告警和记录功能，从而提供系统的安全性。

- 日志审计和报表功能

亚信安全 DeepSecurity 提供全面的系统日志和详尽的报告功能，除了记录自身的各功能日志外，还可以将虚拟主机操作系统日志结合 DeepSecurity 自身日志进行统一的统计和分析，日志系统还可以生成符合国际相关安全规范的报表。

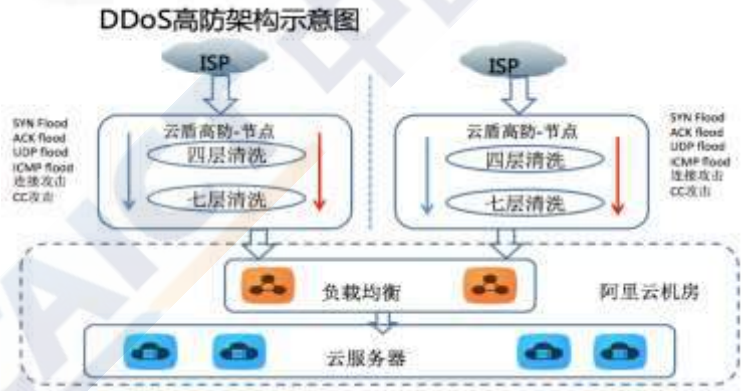
DeepSecurity 通过对日志进行分析可以让管理员跟踪 IT 基础设施的活动，评估服务器数据泄密事件是否发生、如何发生、何时发生、在何处发生的有效方法。

（七）阿里云：基于全球防御体系的大流量 DDoS 防护实践

DDoS 高防 IP 服务是阿里云自主研发、通过专用高防机房提供 DDoS 攻击防护的云安全服务。服务针对互联网服务器（包括非阿里云主机）在遭受大流量 DDoS 攻击后导致服务不可用的情况时，将攻击流量引流到阿里云高防 IP 机房，经过对攻击流量的清洗后将正常业务流量转发至源站服务器，从而确保源站服务器的稳定可用。

1. 超大规模分布式全球 DDoS 防御体系

阿里云在全球范围内升级云盾高防网络，以提高响应速度和稳定性，防御能力近 10Tbps。DDoS 高防 IP 服务突破了现有 BGP 高防防护带宽小、购买成本昂贵等不足，相比传统静态大带宽攻击防御系统的优势体现在灵活的弹性可扩展能力，更好的网络稳定性和交付体验上。在分布式能力上，DDoS 高防 IP 服务全面升级 BGP Anycast 网络，充分利用阿里云全球清洗中心能力，采用智能调度技术将大规模 DDoS 攻击流量自动牵引至距离攻击源最近的清洗中心，同时具备多机房自动容灾的能力。高防 IP 服务也可以为非阿里云内用户提供同等能力的 DDoS 攻击防御。阿里云内用户防御架构如图附 19 所示。



图附 19 阿里云内用户防御架构

2. 精细化和智能化的防御机制

阿里云基于自主研发的云盾产品，为用户提供全面的 DDoS 防护服务，可以防护 SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Query Flood、NTP reply Flood、CC 攻击等三到七层 DDoS 攻击。除了对传统业务提供有效的防御之外，阿里云 DDoS 高防 IP 服务层支持对包括社交类 APP、交易、视频直播和智能物联网等低延迟，高实时性新业务应用的大规模 DDoS 攻击防御。

在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，结合 Web 安全过滤、信誉、七层应用分析、用户行为分析、特征学习、防护

对抗、威胁情报等多种技术，对 DDoS 攻击进行阻断过滤：

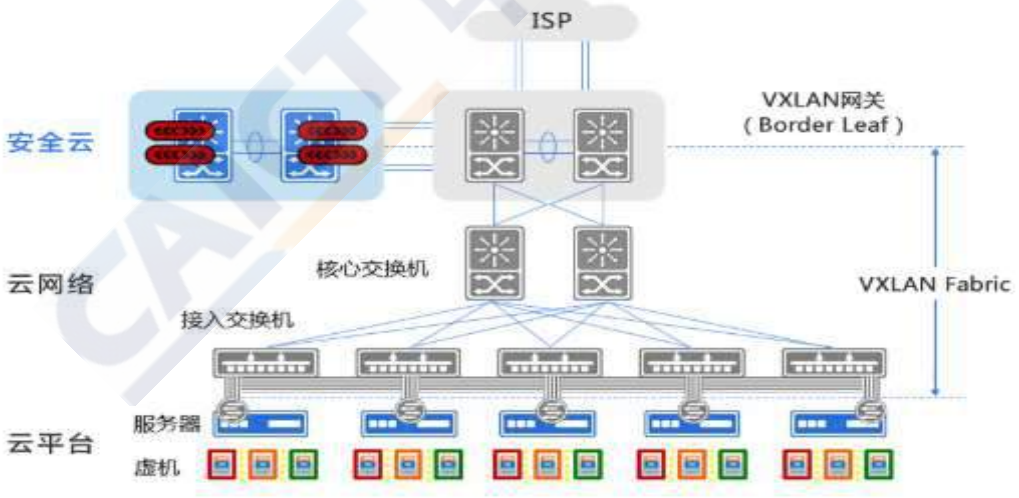
- 精细化。通过对 in/out 双向流量信息的分析，提供精细化、域名级别、session 级别的应用级 DDoS 防护；
- 智能化。摆脱传统基于统计的分析算法，引入了行为识别、机器学习算法和实践，使得防御更加高效和精准；
- 全网威胁情报。基于阿里云安全大数据和全网威胁情报能力，针对全网的恶意 IP 进行持续跟踪，在去除掉伪造 IP 后，系统能根据 IP 信誉库自动过滤掉经常发起攻击的恶意 IP。

3. 防御过程和效果可视化

安全可视化是云安全服务的关键能力，特别是在大流量 DDoS 攻击场景下，对攻击的实时监控显得尤为重要。阿里云 DDoS 高防 IP 服务不断升级可视化能力，实现攻防的数据化、可视化和透明化。阿里云 DDoS 高防 IP 服务提供对攻击完整和详细的记录，一方面可以进行快速有效的实时分析，进一步改进防护效果；另一方面也便于后续取证和溯源，变被动防守为主动对抗。

（八）杭州迪普：基于硬件设备的云数据中心安全防护解决方案

迪普科技提出了以“云安全、硬实力”云数据中心安全解决方案，通过独立的硬件安全设备来解决云网络的安全问题，帮助用户构建自动化部署的安全资源池，为云网络提供全面、弹性、可编排的安全防护能力，如图附 20 所示。



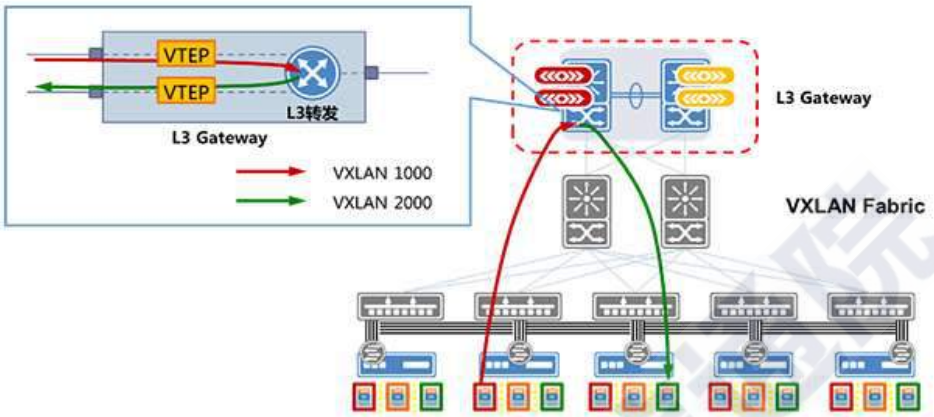
图附 20 方案部署图

- 无缝对接云网络

由于在云环境下，同一物理服务器下的多租户互访默认通过虚拟交换机就能转发，并不通过物理网络设备和安全设备。因此在云环境中东西向安全是一个比较大的难题。迪普科技通过将安全网关与 VXLAN 技术的结合解决了这一问题。

迪普科技 VXLAN 安全网关可以作为 VTEP（VXLAN Tunnel End Point）,即

三层网关，用于对 VXLAN 报文进行封装、解封装，并进行跨 VXLAN 的三层报文转发。在虚拟机和安全网关中，形成一个完整的 VXLAN 网络，处于不同 VXLAN 的虚拟机之间互访必须经过迪普科技安全网关进行转发和控制，从而实现了对于多租户之间的安全隔离。三层网关（L3 Gateway）工作原理图如图附 21 所示。



图附 21 三层网关（L3 Gateway）工作原理图

- 适应多租户的安全虚拟化

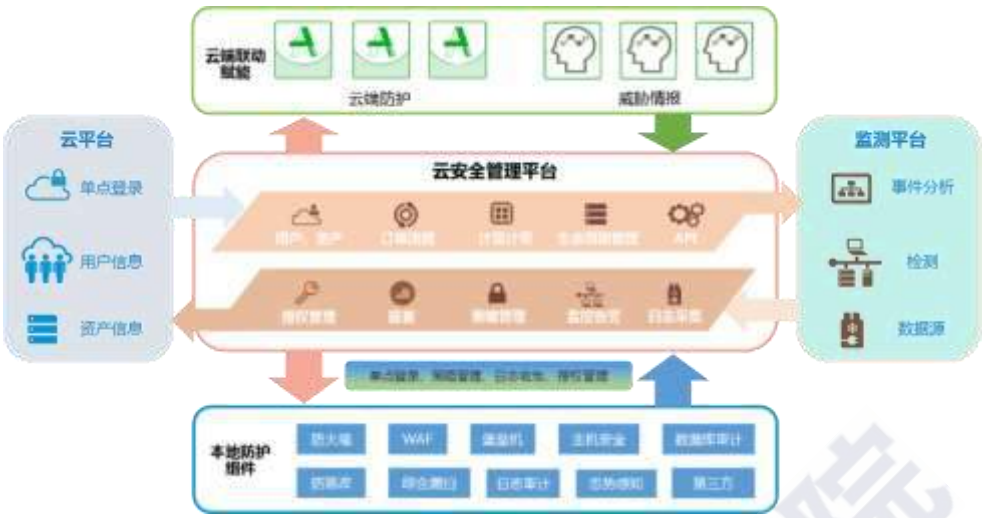
迪普科技使用 N:M 虚拟化技术，将 N 台设备虚拟成一个资源池，再将资源池按需分成 M 台逻辑设备，从而实现针对不同的租户划分出不同的 VSA（虚拟安全设备），可以从 CPU、内存、吞吐量、并发连接数、新建连接数、路由协议等维度进行划分，从而实现 1 个租户、1 个 VSA、1 个配置界面的目标。

- 自动化编排能力

迪普科技的云安全网关全面支持基于 OpenStack 的云管理，用户可以像管理计算、存储、网络资源一样管理迪普的安全设备，实现真正意义上的资源自动配置管理。

（九）奇安信：基于协同联动的云安全实践

奇安信云安全管理平台创新性的融合多种安全技术与云计算技术，可面向云上租户和业务提供全面、定制化的安全服务。该解决方案整体设计以“防范”为中心，基于传统的边界防御技术，提升为由“预防—防御—监测—响应”等技术形成的立体安全防护架构，深入云内，覆盖了云环境中的网络层、宿主机层、虚拟化层、云主机层、应用层、数据层等多层防护。云安全管理平台架构图如图附 22 所示。



图附 22 云安全管理平台架构图

云安全管理平台主要有以下特点：

- 立体联动防御体系

方案遵循“发现”-“阻断”-“取证”-“研判”-“溯源”的防护体系，通过云安全威胁感知系统将原本碎片化的威胁告警、防护状态、云内资产等信息数据结构化并统一整合，并结合威胁情报进行安全预判溯源，通过实时交互可视化技术，将原来未知安全威胁变得可视可管，使安全态势一目了然，最终实现“云端、边界、端点”+“安全可视与感知”的立体联动防御体系。

- 东西向流量的微隔离：

以虚拟主机安全防护为核心，采用软件定义的安全资源池，通过配置 AV、HFW 和 HIPS，实现东西向流量之间的微隔离，构建主机安全防护，重点解决虚拟网络层面的边界防护、虚拟网络可视化等问题，同时实现虚拟机迁移过程的安全策略跟随。

- 安全服务链编排

用户可根据不同业务需求部署不同的安全组件（如 vFW、入侵检测、vWAF 等），按需编排服务节点形成安全服务链，在全生命周期内为应用提供安全服务。

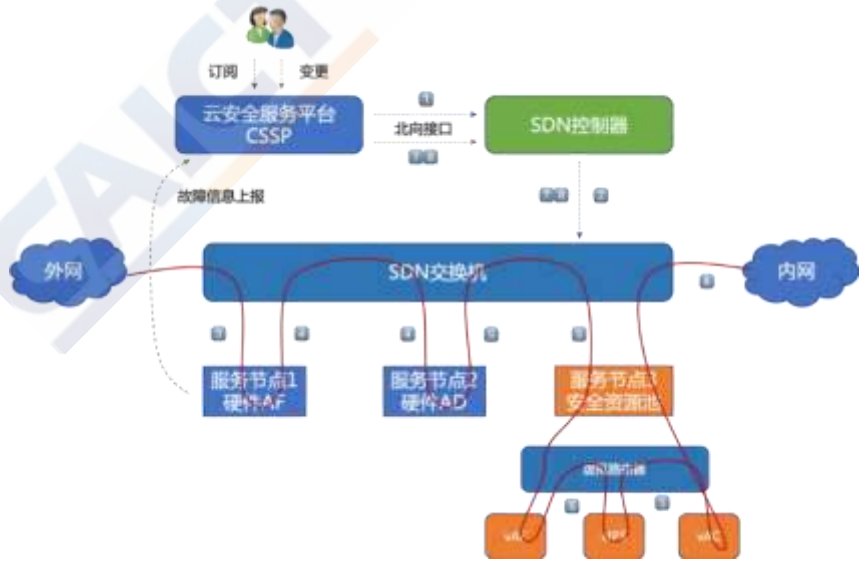
（十）深信服：云安全技术实践

云安全服务链技术是深信服在软件定义安全领域的创新实践之一。云安全服务链是云计算环境下，安全产品服务化、自动化交付的核心技术，能够实现基于用户身份、业务应用类型对网络流量进行按需防护，支持根据不同业务需求将不同的安全硬件或 NFV 节点（如 vFW、入侵检测、vLB 等）按需编排形成安全服务链，在应用生命周期内为应用提供安全服务。技术原理和框架如附图 23 所示：

- CSSP 将用户输入的订阅信息（如用户购买的安全组件及定义的组件顺序）和标识信息（用户五元组和 VLAN 信息），通过北向接口下发给 SDN

控制器；

- SDN 控制器根据用户的订阅信息、标识信息和服务节点的网络配置（如网络设备的接口、VLAN）计算出流表（基于 OpenFlow 协议）下发给 SDN 交换机；
- 当来自外网的数据流第一次经过 SDN 交换机时，SDN 交换机按照定义的流分类规则匹配数据报文，并将其转发到相应的服务链，进入第一个服务节点；
- 从第一个服务节点返回到 SDN 交换机的数据流，SDN 交换机基于入端口、五元组信息或 VLAN 查询流表（基于 OpenFlow 协议），匹配相应的出端口，转发到下一个服务节点；
- 数据流按照服务链定义的顺序在服务节点之间按顺序转发；
- 最后一个服务节点返回到 SDN 交换机的数据流，SDN 交换机基于入端口、五元组信息或 VLAN 查询流表（基于 OpenFlow 协议），匹配服务链出端口，转发到内网；
- 当服务节点状态发生变化时，如服务节点故障停止工作，CSSP 将检测到该变化，并通知 SDN 控制器重新计算流表，下发给 SDN 交换机完成服务链动态更新；
- 当用户订阅信息发生变化时，如服务节点授权到期，CSSP 将检测到该变化，并通知 SDN 控制器重新计算流表，下发给 SDN 交换机完成服务链动态更新。



图附 23 云安全服务链技术架构

附件三

我国企业零信任框架相关实践

（一）山石网科：微隔离可视化云计算安全，云中零信任安全模型

某省某局利用山石云•格实现云计算环境中多个安全域之间的隔离，在私有云中实现了零信任安全模型。

山石云•格，根据不同的微安全域，数据资产被访问的特性，进行了各微分域的隔离，设定了最低授权的访问控制策略。

对于一些新上线的的应用，使用了山石云•格的策略助手的策略学习功能，对应用的访问情况进行观测，并会同应用开发、网络安全相关人员，确定最低授权的访问控制策略，确保零信任思路的贯彻执行。

由于用户最初采用特定虚机名称命名方式与微分域数据资产进行了较好映射。在新增业务虚机时，山石云•格通过云平台 API，动态感知变化，依照既定微分域思路动态调整安全域，为新增的业务虚机匹配相应的防护安全策略，降低配置工作量，及时防护。

山石云•格的可视化功能，对云内虚机进行监控，实现了云内部应用、威胁的可视。在云计算环境下，处于自动化运营考虑，虚机承载业务单一，网络行为理应较为规律，除更便于制定最低应用授权外，也便于观察网络行为，异常行为更便于发现，方便管理员发现潜在未知威胁。

山石云•格集成了 2-7 层的全面防护，同时采用专利引流技术，分布式处理架构，不需要将防护目标的流量引入到外部设备上，在整理实现上也更符合零信任安全模型中网络安全、可视紧密结合，提升处理效率，满足微安全域平行对等互联的思路。

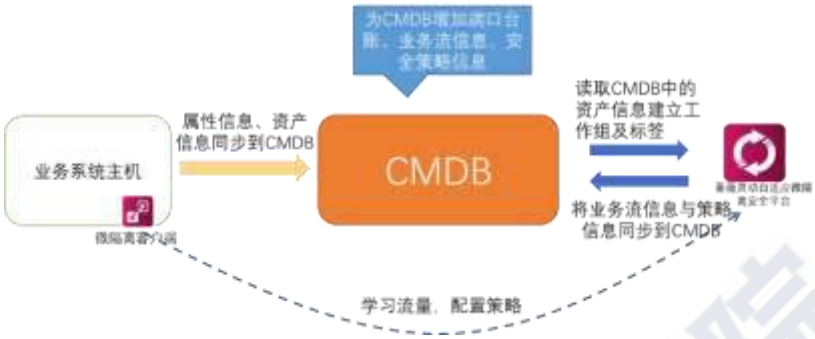
（二）蔷薇灵动：基于微隔离技术的云中心东西向隔离的 DecSecOps 实践

1. 对于已有系统，微隔离与 CMDB 对接，实现业务流学习与精细化策略配置

通过与 CMDB 的对接，将工作负载（承载业务的主机）的属性信息读取到微隔离产品的管理中心上，并自动生成对应的业务组及工作负载的角色标签。通过自动化运维工具批量部署微隔离客户端，通过 IP 作为媒介，安装好客户端的工作负载会自动接入管理中心的对应业务组中并配置相应标签。

微隔离客户端会自动学习工作负载间的访问关系，绘制业务流量拓扑，同时

将学习到的业务关系转换为业务流信息上传到 CMDB 中，即可实现对已有系统的业务梳理。再由业务部门对业务流信息进行审核，审核通过的即可回传至微隔离管理中心，管理中心将确定的业务流信息自动生成安全策略下发到各工作负载之上。基于微隔离技术的 DevSecOps 示意图如图附 24 所示。



图附 24 基于微隔离技术的 DevSecOps 示意图

2. 对于新系统，微隔离与 CMDB 对接，实现安全与业务同步交付

在系统上线时，业务部门需要在 CMDB 中说明新业务内部、新业务与已有业务的业务流信息，微隔离客户端默认安装在操作系统的镜像中。

当新业务上线时，微隔离管理中心会读取 CMDB 中工作负载的属性信息外，还读取业务流信息，管理中心会基于业务流信息自动生成新的安全策略集修改原有安全策略，从而实现业务与安全的同步交付。对于几百上千台虚拟机的环境，这方案可以大幅减少安全策略管理的工作量，并提升内部安全等级。内部业务流拓扑效果图如图附 25 所示。

图附 25 内部业务流拓扑效果图

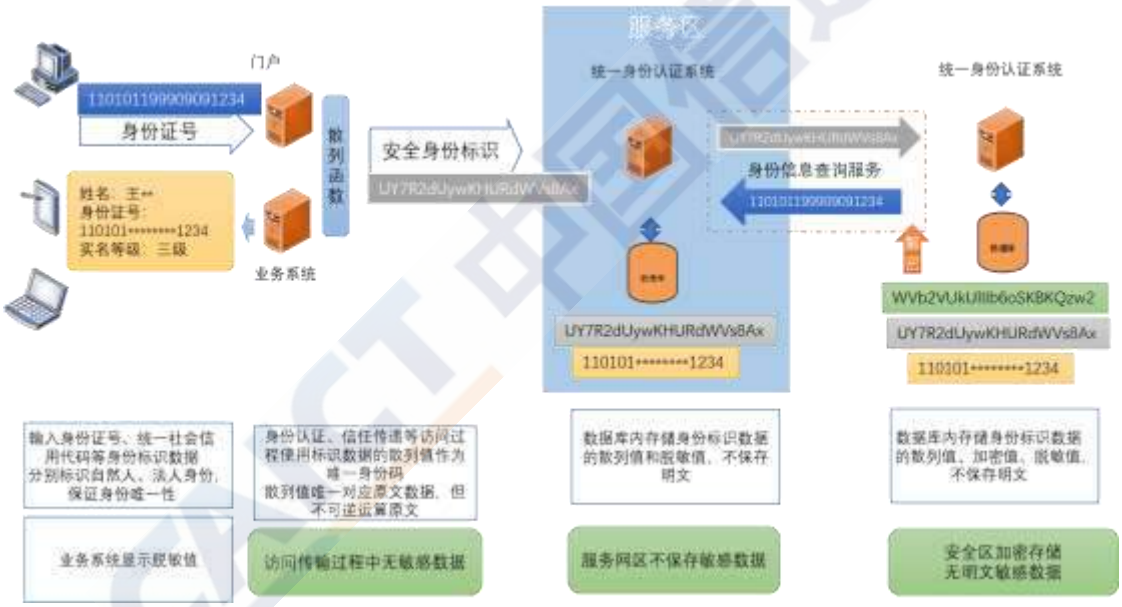
3. 内部流量的分析，与异常行为的发现

通过一段时间对工作负载间的业务流信息的自动学习，可得到业务流基线，通过业务流生成安全策略后，任何偏离基线的访问均会被记录并阻断，基于阻断信息，可以发现内部的异常情况。

同时管理中心还记录云中心内部工作负载间的访问信息，用户可以基于多个维度进行搜索和溯源。

（三）亚信安全：身份隐私数据的零信任访问控制实践

亚信安全采用去标识化和数据脱敏技术为基础，以零信任访问控制机制为核心，构建了一套安全的身份数据访问控制机制。首先在数据层面上，贯彻数据最小化原则，控制身份数据适用范围，对源头即开始对原始隐私数据进行处理和保存，在数据传输、处理、存储等所有环节中不使用原始数据。具体方法以去标识化方法将原始身份标识数据进行散列化处理得到一个安全身份标识。此标识可以确定一个自然人或法人的确切身份、可以进行登录认证等业务操作，又能不使用真实身份信息。同时，对于非标识的普通数据进行脱敏。由此，对于身份隐私数据，按照最小化原则，约定能使用安全标识和脱敏数据进行处理的业务，一律使用安全身份标识。这样在大部分业务中，实际上不使用真实身份数据，杜绝了身份数据泄露的最主要源头。融合身份认证管理如图附 26 所示。



图附 26 融合身份认证管理

对于少部分需要原始身份信息的业务，可以使用原始身份库中的信息，但必须经过授权。授权必须经过认证，而且是零信任原则下的“认证一切”式认证，在设备认证层面，采用了以密钥分割技术为支撑的手机端认证；对于人的认证则支持手机短信、生物特征识别等多种认证方式。满足人机一体的认证后才能获得相应访问权限，同时保持“持续认证”，例如登录时间较长而访问令牌仍未超时是，将启动二次认证。在访问重要业务场景时，也将发起二次认证，保证当前操作由真实身份拥有者进行操作。

亚信安全还加入了认证行为风险防控机制，对于用户的身份行为进行管控，及时发现风险，启动相应策略，保障用户业务和身份安全，也符合了零信任机制

中情境感知的核心原则。

（四）阿里云：基于完整可信框架的零信任实践

阿里云零信任模型依靠云平台硬件安全中的可信计算能力，通过自研开发基于硬件的可信服务，实现云上的软件栈可信。同时，基于统一身份管理服务（IDaaS）确保企业用户对云应用的可信访问，从而达到企业云上整体安全可信升级的目标。

1. 可信根

阿里云可信根采用在商业和产品化上成熟的 TCM，通过使用装有 TCM 可信芯片的可信服务器作为系统的可信根逐级实现云平台以及其上业务的可信。

阿里云开发 TCM 虚拟化（vTCM）实现虚拟机可信。云平台物理宿主机上一般需运行多个虚拟机，为保证对虚拟机的度量，需要同时有多个 vTCM；同时虚拟机会因业务的需要而迁移，为保证虚拟机度量的延续性，其可信相关的安全管理数据如最后的 PCR 值等应同步迁移到目标主机上。阿里云 TCM 虚拟化（vTCM）很好地解决了上述需求。云平台可信根实现框架图如图附 27 所示。

图附 27 云平台可信根实现框架图

2. 芯片级加密技术的可信计算

阿里云 2017 年便与英特尔联合发布了基于芯片级的 SGX 加密计算技术(即机密计算技术)，提前布局，用最前沿的技术保障云上客户数据安全。基于 Intel SGX 加密计算技术，阿里云为云上客户提供了系统运行时的可信能力，云上开发者可以利用 SGX 技术提供的可信执行环境，将内存中的关键代码和数据保护起来，即使具备更高特权的系统组件包括 BIOS、虚拟化底层、操作系统内核，以及高特权进程也都无法获得关键代码和数据，让客户可以摆脱对云平台的依赖，通过拥有云上的可信执行环境，防止数据被窃取或被篡改。

3. 可信身份认证

阿里云应用身份服务（IDaaS）是阿里云为企业用户提供的一套集中式身份、权限、应用管理服务，帮助企业整合部署在本地或云端的内部办公系统、业务系统及三方 SaaS 系统的所有身份，实现一个账号打通所有应用服务。阿里云应用身份服务 IDaaS 不是简单把企业的身份管理系统搬上云，是通过云原生的能力来去重塑整个企业的身份认证架构，实现基于云的统一身份认证授权体系，形成企

业新的安全边界。

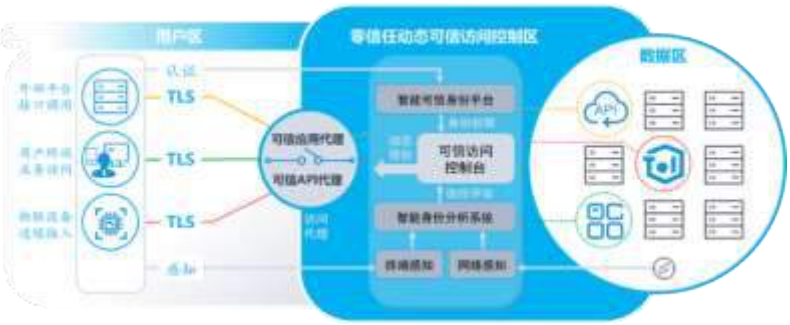
IDaaS 具有如下特点：

- 完整：不仅包括云上、云下（企业本地数据中心）、混合部署、跨云多云等各种形态，同时也包括对资源、应用和数据全面覆盖；
- 统一：一套账号体系打通企业内部多个应用系统，实现单点登录，统一用户登录，统一的身份认证，统一的行为审计，统一资源访问管理；
- 集中：集中认证和授权管理。

（五）奇安信：零信任身份安全解决方案

奇安信零信任身份安全解决方案基于“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力，构筑基于身份的动态虚拟边界产品与解决方案，旨在提供全面身份化、授权动态化、风险度量化、管理自动化的新一代网络安全架构，如图附 28 所示。

- **以身份为基石**：即为网络中的人和设备赋予数字身份，将身份化的人和设备进行运行时组合构建访问主体，并为访问主体设定其所需的最小权限。身份是物理世界的人/物/系统等实体在数字世界的唯一标识和属性集合，是物理世界的实体在数字世界的对等物。
- **业务安全访问**：零信任架构关注业务保护面的构建，即：针对要保护的核心业务资产构建安全访问的屏障，这些业务包括应用、服务、接口等等。通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小限度的开放，所有的业务访问请求都应该进行全流量加密和强制授权。
- **持续信任评估**：即通过信任评估引擎，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别并对信任评估结果进行调整。
- **动态访问控制**：动态访问控制是零信任架构的安全闭环能力的重要体现。通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。



图附 28 奇安信零信任身份安全解决方案典型逻辑图

奇安信零信任身份安全方案核心组件包括可信访问控制台（TAC）、可信应用代理（TAP）、可信 API 代理（TIP）、可信终端感知系统（TESS）、可信网络感知系统（TNSS）、智能身份分析系统（IDA）、智能可信身份平台（IdAM）等，通过在用户区、数据区部署安全访问控制区构建动态可信访问控制平台，保障主体对客体业务、数据访问的安全可信。

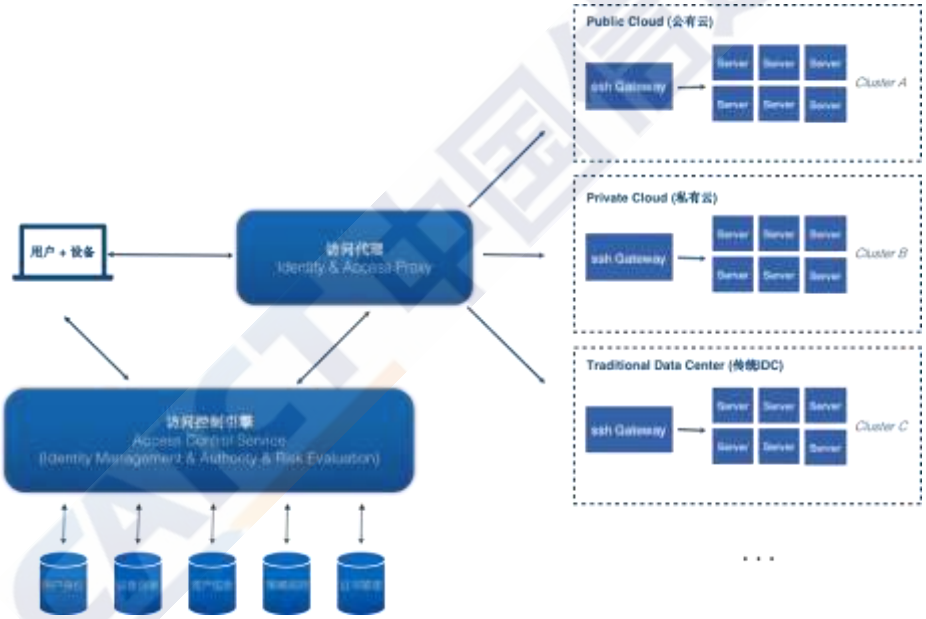
- **可信访问控制台(TAC)：**为 TAP/TIP 提供动态访问控制和集中管理能力，针对企业的各个业务访问场景，实现了访问控制策略统一配置管理、WEB 应用和 API 服务集中管理、用户认证与动态授权、风险汇聚关联、应用审计等功能。可信访问控制台是弹性动态访问控制体系的核心组成部分，是联动各个子系统的控制中心。
- **可信应用代理系统(TAP)：**针对企业多个应用的访问控制需求，实现了应用的分层安全接入、一站式应用访问、应用单点登录、应用审计等能力。同时，可信应用代理系统也是弹性动态访问控制体系的重要组成部分，用于用户/终端和业务应用之间的安全访问，是弹性动态访问控制体系的访问控制策略执行节点。
- **可信 API 代理系统(TIP)：**针对 API 服务的安全保护需求，实现了 API 接口的统一代理、访问认证、数据加密、安全防护、应用审计等能力。同时，可信 API 代理平台也是以弹性动态访问控制体系重要组成部分，用于业务应用/应用前置和后台服务之间的安全 API 调用，是弹性动态访问控制体系的访问控制策略执行节点。
- **可信终端感知系统(TESS)：**提供终端环境的安全状态，为智能身份分析系统(IDA)提供实时的终端可信度的判断依据。
- **可信网络感知系统(TNSS)：**提供网络流量环境的可信状态，为 TAC 提供实时的可信度判断的依据。
- **智能身份分析系统(IDA)：**基于 TAP/TIP/TAC 访问日志、可信环境感知上报的风险、其他外部分析平台上报的风险进行综合风险关联判定，利用大数据分析和人工智能技术，构建信任评估模型进行持续风险评估，为动态访问控制提供信任等级评估。
- **智能可信身份平台（IdAM）：**提供身份安全基础设施，提供全面的身份管理、权限管理和身份治理服务。为可信访问控制台提供身份及权限信息。

（六）腾讯：互娱海量服务器集群身份和访问管理安全运维解决方案

腾讯基于零信任安全的理念，研发出一套完整的身份和访问安全管理解决方案，满足等保 2.0 中对于安全计算环境的身份鉴别、访问控制、集中安全审计等要求，并能协同安全边界防护及访问控制，实现框架如图附 29 所示。

解决方案特性如下：

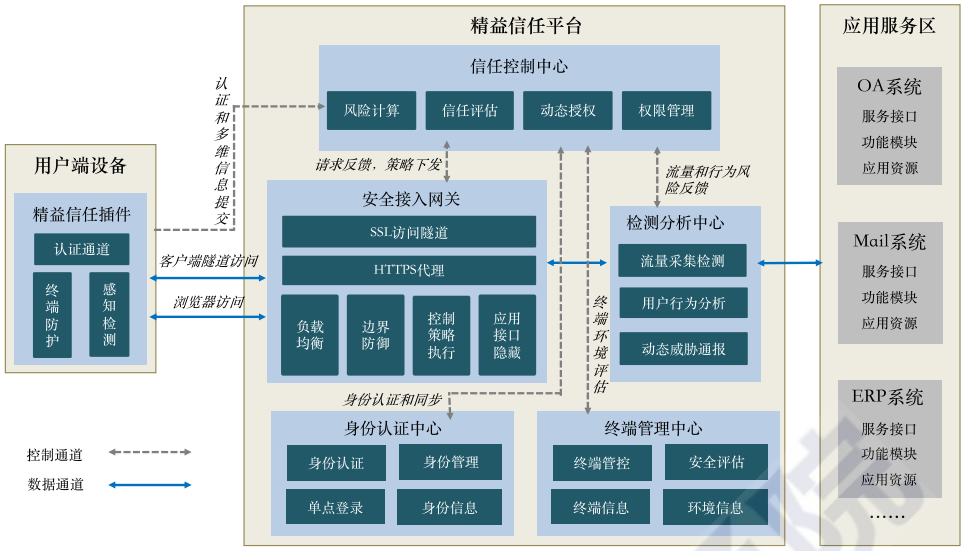
- 面向多云大规模集群设计。不管是公共云、私有云、混合云还是多云或者传统 IDC，为所有云访问管理提供统一的解决方案。
- SSO 登录 + 多种权限管理模型。支持企业级标准（SAML/OAuth 认证）SSO，统一身份认证；通过 RBAC/ABAC 配置相应策略，最小化访问控制权限。
- 使用动态证书替代传统静态票据。使用无密码动态临时证书方式，解决传统静态密码票据泄露被窃取风险。
- 无 Agent，极易实施，可靠性高。基于 OpenSSH 原生，无需安装 Agent，无需额外系统依赖，可靠性高。
- 原生登录，跳板机无感知。兼容用户习惯，登录体验；无需一级级跳板机跳转，一键直达目标机器。
- 会话回放，操作审计，异常发现。会话完整记录，操作追溯审计，结合 AI，识别高危、异常行为。



图附 29 身份和访问安全管理实现框架

（七）深信服：零信任安全技术实践

深信服基于精益信任理念，对精益信任安全访问架构进行了技术实现。精益信任安全访问架构如图附 30 所示。



图附 30 精益信任安全访问架构

精益信任安全访问架构包含精益信任平台和精益信任插件。其中精益信任平台部署于应用服务区前端，控制对应用服务区的访问行为。平台由 5 个模块组成，分别是信任控制中心，安全接入网关，身份认证中心，终端管理中心和检测分析中心。5 个模块和精益信任插件的功能分别是：

- 信任控制中心：基于身份、环境、行为、设备信息，信任控制中心负责进行信任的评估和权限管理。
- 安全接入网关：可信接入网关接收信任控制中心下发的策略，实现访问行为的控制。
- 身份认证中心：身份认证中心存储用户的身份信息，与权限控制管理系统对接，进行用户身份的核对和更新。并与后端业务系统对接，实现身份管理、单点登录、联邦认证等功能。
- 终端管理中心：终端管理中心存储终端设备信息，包括 IP、硬件特征码、操作系统、安全软件、应用软件、漏洞等信息。
- 检测分析中心：检测分析中心对用户访问行为和流量进行检测，发现异常、攻击行为和恶意流量。
- 精益信任插件：部署于用户端的个人电脑（PC）或移动终端上，实现用户端设备防护、环境感知，并建立对接精益信任平台的认证通道。

基于上述基本模块，精益信任安全访问架构实现了访问建立前，默认所有用户和设备不可信。同时信任的建立基于对用户身份、设备信息、环境信息的综合评估。业务交互过程中，每一个交互流量都带有与用户和设备身份绑定的标识，以防止恶意攻击。并持续监测设备、用户的多源上下文信息（设备信息、行为信息、环境信息），进行风险评估。并基于风险评估结果，对风险和当前的信任等级进行比较，持续调整信任等级。

同时，在降低落地障碍方面，精益信任安全访问架构具有以下技术特点：

- 支持代理模式与隧道模式：对于很多采购了 VPN，内部业务系统 C/S 和 B/S 架构并存的客户，精益信任安全访问架构同时支持 B/S 架构下的代理模式，与 C/S 架构下的隧道模式，实现了对现有 VPN 设备和应用系统的兼容。同时，VPN、HTTPS、SSH 等访问协议下，均可以实现风险/信任的持续评估和动态控制。
- 私有部署和云化部署：精益信任安全访问架构中的平台，支持本地独立部署与云端部署。云端部署模式下，平台模块通过网络功能虚拟化形式在公有云或私有云平台中实现，仍以上述精益信任的保护方式对云内资源提供防护。
- 按需部署组件：精益信任平台中包含多个模块，共同实现风险/信任的持续评估和动态控制。整体平台支持模块的可裁剪。当缺失某个模块时，信任控制中心承担此模块的部分功能，用户的业务访问仍然可以进行，并仍具有精益信任控制功能。
- 风险/信任传递标准化：精益信任安全访问架构中，通过在信任控制中心中实现一个风险/信任接口标签库，来支持对多厂商、多类型设备的兼容，实现信任建立和持续评估过程依靠模块间广泛持续的互动和通信。

附件四

我国企业“人工智能+安全”相关实践

（一）三六零：人工智能系统安全检测系统实践

人工智能系统安全检测系统是一款检测 AI 系统自身安全风险的产品。依靠 360 安全大脑强大的数据平台，以及 360 安全团队在安全领域中的技术积累，该系统旨在为用户提供人工智能系统中安全风险检测的结果，包括漏洞 POC 及报告。

1. 整体框架

本方案技术路线由基础分析、安全风险检测两部分工作完成。基础分析主要实现包括组成成分分析、攻击面分析。其中组成成分分析实现对不同 AI 系统中的框架及依赖组件的关联性分析；攻击面分析实现对可能受攻击的 AI 框架及依赖组件进行多维度的脆弱性分析。本工具将对以上分析的结果进行存储和可视化展示。安全风险检测包括了已公开安全风险检测和未公开安全风险检测。其中已公开安全风险即 NDay 漏洞，而未公开安全风险检测即对各个开源框架及第三方组件进行 0Day 漏洞挖掘。安全风险检测的结果输出为漏洞 POC 及报告。

2. 技术原理

组成成分分析。相当数量深度学习系统直接使用第三方组件来实现某些功能，如在 Caffe 中，直接调用 OpenCV 图像处理库中的函数来进行图像数据的处理。因此，除了深度学习系统本身框架的功能模块，还需要对各框架所使用的第三方组件进行分析。

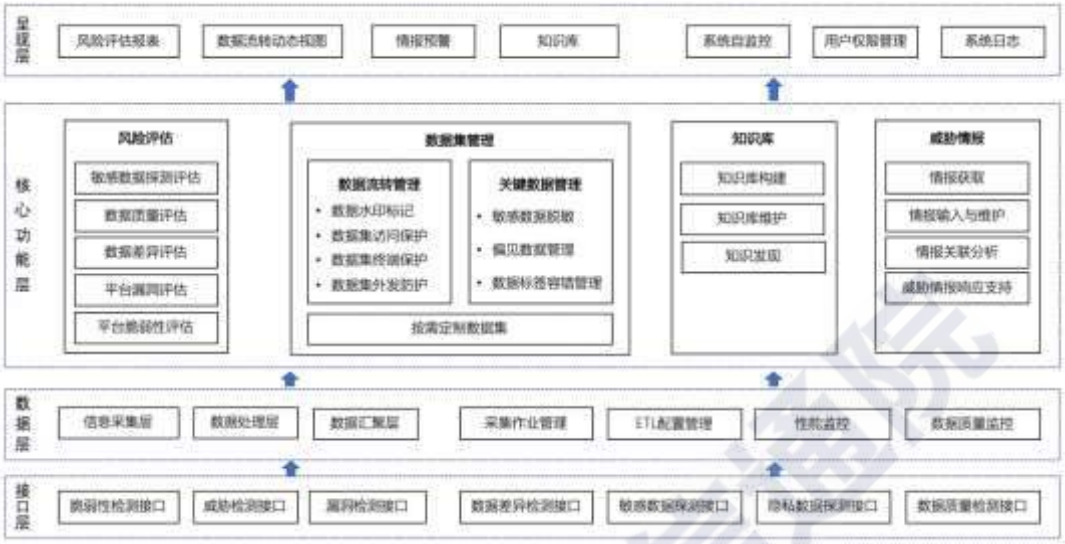
攻击面分析。当深度学习系统与外部环境进行交互时，可能会引入未知的安全风险。如在输入数据处理阶段，可能会存在数据劫持、数据替换等操作，从而使得深度学习系统出现识别错误；甚至当数据处理代码中存在安全风险时，攻击者可以通过构造恶意输入，控制整个深度学习系统；在输入数据或结果数据进行传输过程中，攻击者也可以通过中间人攻击等方法控制人工智能系统的输出结果。

已公开安全风险检测。根据对主流深度学习系统的基础分析结果等数据信息，重点对涉及攻击面的主流深度学习框架及第三方组件的安全风险进行检测。这些安全风险普遍存在于外部环境交互的模块中。

未公开安全风险检测。将对 AI 系统中外部环境交互相关的模块、第三方组件进行漏洞挖掘。在检测技术方面，主要采用多种漏洞挖掘技术相结合的方式进行检测，如模糊测试、符号执行、静态分析等。

（二）上海观安：基于人工智能数据安全风险评估的实践

数据安全风险和隐私保护成为人工智能系统在开发和应用过程中面临的严峻安全挑战，而人工智能需要数据来建立其智能。基于人工智能数据安全风险评估总体架构图如图附 31 所示。



图附 31 基于人工智能数据安全风险评估总体架构图

1．基于人工智能数据安全风险评估

风险评估模块基于各检测工具的检测结果和数据进行综合的数据安全风险评估。该模块的功能包括：敏感数据探测评估功能、数据质量检测评估功能、数据差异检测评估功能、AI 平台漏洞检测管理功能以及 AI 平台脆弱性检测管理功能。

2．人工智能数据安全基线

根据自研标准、各类监管政策、相应的国家及行业标准规范以及国内外的优秀实践，建立多样化的安全检查基准及不同强度的策略标准指标体系，形成一系列适用于各类人工智能应用场景的数据安全基线，实现多基线动态比较，自动生成基准差异和全局安全态势，服务于监管部门、产业发展部门、人工智能重点应用单位、开发厂商等，达到准确掌控人工智能应用安全趋势的目标。支持产业、多样化应用场景、可用户定制的安全基线设置和动态比较。

3．产品形态

人工智能数据安全风险评估平台，以产品服务的形式为用户提供人工智能平台上的数据安全检测评估，包括平台上威胁数据安全的检测以及数据上的安全检测，包括敏感数据探测评估功能、数据质量检测评估功能、数据差异检测评估功能。

4．技术应用以及创新点

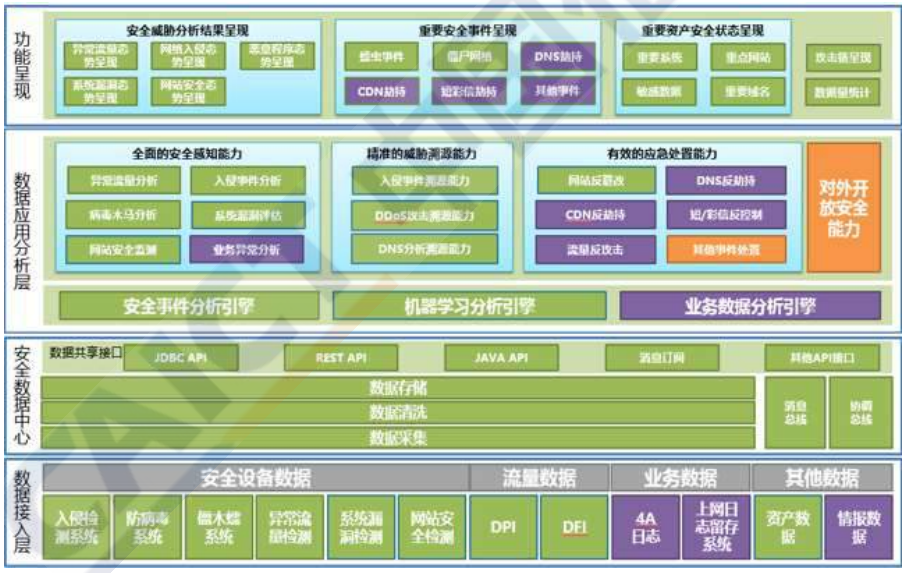
- 敏感数据探测评估功能。根据自定义规则建立的敏感数据库样本不断训练出自学的人工智能敏感数据探测功能模块：首先搜集敏感信息的文本

数据，利用人工标注平台，标注敏感数据类别；然后利用对应的人工智能模型训练标注模型，最后部署敏感数据检测模型。

- 数据质量检测评估功能。首先采集需要评估平台的目标数据，制定对应的数据质量标准基线，然后对需要评估平台的数据进行质量评估，最后根据评估结果生成对应的数据质量检测评估报告。支持对数据质量检测评估出数据中是否含有偏见数据等，生成数据质量评估报告
- 人工智能数据安全知识库。对各国人工智能数据安全领域的伦理规范、法律法规、政策、标准、最佳实践等进行量化分析，从而建设专业的政策数据库；以高质量的知识库建设，综合外部实时动态信息，实现情报检索、专利分析、态势简报等功能，输出向社会和产业共享的、可以在本平台查询的人工智能数据安全知识库。

（三）绿盟：基于大数据的安全态势感知分析和溯源系统实践

绿盟安全态势感知分析和溯源系统采用大数据技术作为底层支撑，解决了传统安全分析中数据分析的性能瓶颈问题，实现了实时安全数据分析功能，完成了自主灵活的安全可视化目标。安全态势感知分析和溯源系统如图附 32 所示。



图附 32 安全态势感知分析和溯源系统

功能呈现层包括首页、安全态势视图与报告、安全告警、一键处置等，同时提供原始日志与标准化日志的搜索入口，及本系统的系统管理入口。数据应用分析层内置了针对外部安全威胁的分析能力，提供了多种安全分析场景。安全数据中心层，实现各类安全数据的采集、处理、汇聚、存储、检索能力，并向上提供数据订阅接口，以接口形式向安全态势感知的分析提供输入数据。数据源层描述安全数据中心层的数据来源，将数据分为四类：安全设备数据、流量数据、业务数据、其他数据。

- 数据采集、清洗及存储。采用 ETL 对数据统一清洗，数据 ETL 程序从

kafka 队列中批量获取数据，送入 ETL 模块中，调度引擎通过调用 ETL 模块进行数据处理。

- 安全威胁分析感知。利用大数据技术对多源异构数据进行获取、理解、分析，实现对系统安全的集中呈现、态势感知、攻击溯源、以及对威胁事件的预警通报功能。
- 入侵事件全面溯源。入侵事件溯源主要依据攻击链分析模型，通过分析各个网络安全设备收集的安全日志和流量日志生成网络安全事件，进行正反双向推理，正向推理预警潜在威胁，反向推理还原攻击情景。攻击链挖掘程序在网络安全事件的基础之上，按照目的资产的维度将各个安全事件进行聚合，并对应到攻击链的各个阶段，从而发现当前网络中的脆弱主机。网络安全管理员通过分析攻击链的结果，可以了解整个网络当前的安全态势，并且有针对性的对脆弱资产进行加固，提升网络的安全性和抗攻击能力。
- DDoS 攻击溯源。DDoS 攻击溯源基于对 Flow 数据的解析处理，实现对特定的“外到内”和“内到外”DDoS 攻击进行分析和事件追溯。以五元组数据和资产为基础，为门户展示提供数据支撑。另外，基于对流的自学习结果，可分析出 DDoS 的僵尸网络攻击源与 C&C 主控网络。通过数据采集解析引擎对全网 Flow 数据和探针日志进行解析，在高速内存数据库的基础上运用一系列溯源与数据挖掘方法，进行安全事件的追踪溯源，最后通过可视化引擎呈现溯源结果。
- 安全威胁可视化呈现。在充分采集、存储、分析及模型匹配数据的基础上，研究并利用动态智能呈现技术，实现安全场景建模可视化、全文检索、威胁可视化、安全综合报表等符合移动 IT 安全运维相关功能。
- 安全事件归并及提炼。从安全事件分析角度，并不是次数越多的事件威胁越大，而是应该基于安全事件分析引擎，从海量安全告警日志中提炼出更有价值的事件。

（四）威努特：基于智能 Fuzzing 框架的工控漏洞挖掘实践

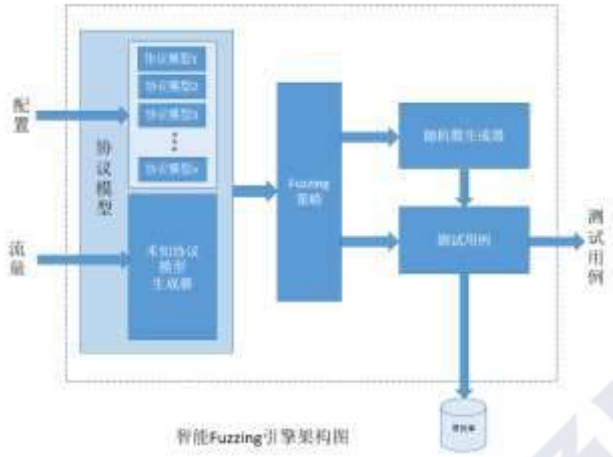
1. 面向工控协议的模糊测试

威努特提出了基于状态的工控协议测试方法，并发布工业控制系统漏洞挖掘平台，采用智能模糊测试（Fuzzing）技术，利用工控协议的状态机进行状态引导，提高了模糊测试命中率与覆盖率，提高了工业网络的漏洞挖掘准确度。

基于生成的（Generation-based）模糊测试（Fuzzing）测试，根据已知的协议、接口规范进行建模，生成测试用例，并且通过随机生成算法，运用合适的策略，进行针对性扰动，来进行遍历程序分支，挖掘漏洞。支持 Modbus TCP、Goose、MMS、SV、PROFINET、IEC104 等工业控制协议。

基于变异的（Mutation-based）模糊测试方法的核心是学习已有的数据模型，

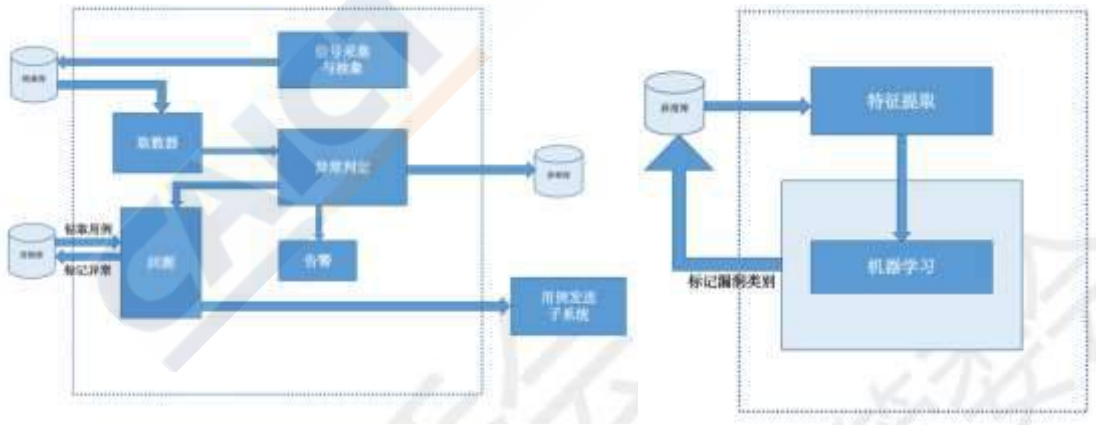
基于已有数据及对数据的分析，再生成随机数据做为测试用例。智能 fuzzing 引擎架构图如图附 33 所示。



图附 33 智能 fuzzing 引擎架构图

2. 面向工控设备固件的漏洞分析

威努特通过对 PLC 固件进行逆向，获取固件信息后对固件进行修改从而完成对 PLC 的攻击；通过分析嵌入式设备固件特点，从漏洞利用的角度分析固件的攻击面，提出一种基于污点分析嵌入式设备固件模糊测试方法，获取程序运行内部对输入数据的处理信息，从根本上理解嵌入式设备的运行逻辑，从而提高对嵌入式设备漏洞挖掘或者攻击的准确度。异常检测引擎和漏洞画像引擎如图附 34 所示。



图附 34 异常检测引擎和漏洞画像引擎

（五）阿里云：基于大数据深度学习引擎的 WAF 防护实践

阿里云云盾 Web 应用防火墙（Web Application Firewall，简称 WAF）基于云安全大数据能力，内置 AI 安全引擎，用于防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器插件漏洞、木马上传、非授权核心资源访问等 OWASP 常见攻击，过滤海量恶意 CC 攻击，避免客户网站资产数据泄露，保障网站的安全与可用性。

阿里云 WAF 已经在全球建成 16 个分布式部署的数据中心，内置近千条针对各类应用的防护策略，建立起了一套多层次多维度智能化的漏斗防御模型，可以为遍布全球的客户提供云端一体化的 Web 应用安全解决方案，有效保障客户在网络威胁攻击下的业务数据安全。阿里云 WAF 已获得国家互联网应急中心、IDC、Gartner、Forrester、Frost& Sullivan 等多个国内外知名机构高度认可。

1. 安全 AI 内核引擎

不同于传统的基于规则检测的安全产品，阿里云 WAF 内嵌一颗安全 AI 内核。通过在每一层中部署不同的机器智能模型，将威胁流量进行分层治理，各层之间的模型各司其职、各体自洽、各级联动，共同协同形成了一套对抗应用层基础威胁和黑客攻击的决策智能体。

- 主动防御：主动防御算法通过无监督学习的方式针对域名的正常访问流量进行深度学习，从而定义正常访问模式，自动化生成自适应于该域名的安全策略，实现「千站千面」的智能防护模式，有效抵御未知威胁；
- 深度学习攻击检测：阿里云自主知识产权的两段式 Web 攻击检测框架，Locate-Then-Detect（LTD）。通过两个深度神经网络的结合 PLN（Payload Locating Network 攻击载荷靶向定位网络）与 PCN（Payload Classification Network 攻击载荷分类网络），可以准确定位恶意攻击所在位置，精准识别其类型，首次解决了深度学习在 Web 攻击检测领域的结果可解释性难题，相关技术创新入选国际人工智能顶级学术会议 IJCAI 2019；
- 云盾防爬实时防控平台（Pluton）：基于马尔科夫、LSTM 等众多机器学习模型，通过对云上海量会话序列进行跨域、多业务维度且全网协同分析，在关键业务接口上进行毫秒级风险判断和防控，异常业务（如恶意占座等）识别率达到 99.98%，可在出现攻防对抗时自动学习到新的绕过 pattern 并自动更新算法参数，依靠智能化技术对抗专业黑灰产团伙。

2. 大数据威胁情报能力加持

在大数据威胁情报能力的加持下，阿里云 WAF 可以实现：

- 全网威胁情报驱动自动化响应。云上攻击、信誉情报共享，针对高危 Web 0DAY 漏洞自动化更新防护策略；
- 攻击可视化。秒级实时在线检索千万业务请求，对攻击事件、攻击流量、攻击规模的全面和集中管理统计，助力用户实时评估当前网站业务安全状况；
- 智能数据风控。帮助用户发现和防御网站关键业务（如注册、登录、活动、论坛）中可能发生的欺诈行为。

（六）启明星辰：基于 UEBA 技术行为检测的实践

V-UEBA 高级威胁类模型检测算法参考业界领先攻击链框架模型，基于行为

模式分析来发现高级威胁关键环节的异常行为和识别攻击。产品提供预置检测分析算法模型，包括 DNS 异常类、C&C 连接类、内部横向移动类、扫描类、DDoS 类、数据收集类、web 攻击类、恶意活动类、僵木蠕等模型。

V-UEBA 系统异常用户类模型主要针对人员、账号等行为进行分析，发现异常访问、违规操作、可疑账号、数据泄漏等潜在风险。用户异常行为分析参考了 5W1H（Who 人员、When 时间、What 对象、Where 地点、Why 原因、How 方法）分析法，从多个维度自学习正常行为基线、发现与正常行为基线的偏离。

算法模型是利用机器学习与统计构建，基于已获取的海量企业网行为数据，建立正常行为模型，对正常行为的偏离识别为异常行为。建立正常行为模型包括基于机器学习形成的正常聚类、基于统计形成的正常分布等。UEBA 行为检测技术框架如图附 35 所示。

图附 35 UEBA 行为检测技术框架

异常行为检测与分析过程：

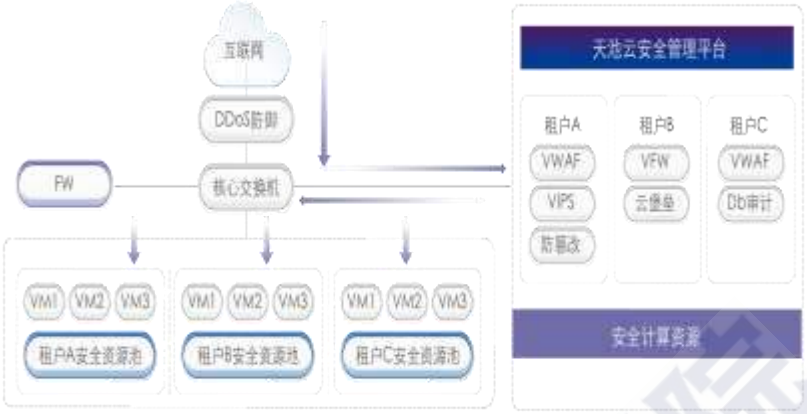
- 采集每个用户、设备等产生的行为数据；
- 建立行为基线、用户画像、设备指纹等常态信息；
- 发现行为与基线偏离，视为反常/可疑；
- 以常态信息、行为上下文信息、情报等数据，作为进一步分析的辅助信息；
- 确定异常行为，给出依据供研判。

（七）安恒：电子政务平台智能安全运营中心

安恒采用智能安全运营中心方案，利用安全资源池的方式智能分配安全能力、利用大数据智能分析平台实现深度安全分析和溯源取证、利用云端监测和安全服务，实现整体云平台的安全运营。

安全防护和监测能力采用安全资源池的方式，根据云租户业务需求自主设置

安全策略集，包括定义访问路径、选择安全组件、配置安全策略。云资源池部署拓扑图如图附 36 所示。



图附 36 云资源池部署拓扑图

- 智能弹性分配安全能力

平台将安全能力以资源池的方式提供，利用智能分配调度算法，为不同的租户和系统分配安全能力，并支持以集群的方式横向快速扩容资源池能力。

- 智能安全分析

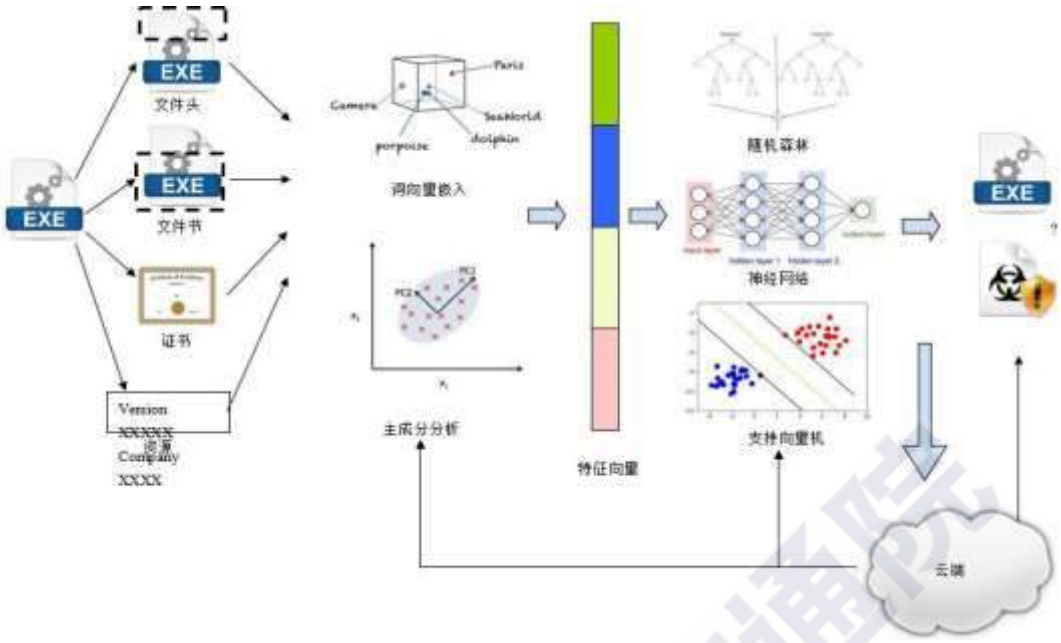
通过 AiLPHA 大数据智能安全的机器学习来发现潜在的入侵和高隐蔽性攻击，预测即将发生的安全事件。通过智能运营中心，实现与安全防护设备形成联动能力，如：FW、WAF、IPS 等，如发生攻击事件，大数据平台可以与防火墙设备联动，自动安全访问控制策略下发至防火墙设备，第一时间组阻断掉攻击者的连接。

- 安全数据集中管控

通过内容分析技术、密码技术、数据防泄漏技术、数据脱敏技术和安全审计等数据安全技术的应用，切实保障数据采集/产生、数据传输、数据存储、数据处理、数据交换到数据销毁的全生命周期安全，为落实数据安全制度规程、实现数据安全防护的总体目标提供技术手段和工具，实现动态的应对数据安全风险。

（八）深信服：安全智能检测引擎的实践

SAVE（Sangfor AI-based Vanguard Engine）安全智能检测引擎优势在于其泛化能力，能够做到在不更新模型的情况下识别新出现的未知病毒。比如影响广泛的 WannaCry、BadRabbit、GlobeImposter 等勒索病毒的未知家族变种，SAVE 在采用旧引擎情况就能实现准确检出，检出率高出业界同类产品。同时基于云+端联动，深信服安全云脑在云端进行持续训练和模型修正，使 SAVE 能够持续进化，不断更新模型并提升检测能力。SAVE 引擎检测原理如图附 37 所示。



图附 37 SAVE 引擎检测原理

SAVE 引擎检测原理如上图 37 所示。基于多文件头、文件节、文件行为等多维信息的综合分析，利用随机森林、深度神经网络等 AI 算法，实现对病毒文件的高为特征提取和综合判定。SAVE 的技术特点有：

- 高层特征自动提取

基于对病毒演化本质的深入理解，SAVE 通过深度神经网络等多种机器学习算法自动提取高层次特征。通过学习海量的正常文件样本和病毒文件样本，它能自动地、逐层地凝练更高层次的特征。比起只利用字节特征的传统方案形成明显优势，SAVE 具有很强的泛化能力，能更好的识别未曾见过的病毒样本，抵御抗病毒变种和新病毒家族等未知威胁。

- 精细特征工程

SAVE 引擎决策模块也集成学习框架，综合了深度神经网络、随机森林、支持向量机等多个机器学习决策模型，基于人工智能专家的有效调优，对检测模型进行有效优化，以实现文件的精确检出。

- 持续演进

除了使用 AI 技术大幅提升检测能力，SAVE 还在云端通过生成对抗网络(GAN)，采用“左右互搏”的方式持续学习，增强模型健壮性和检测能力。GAN 框架中的“生成器”模块能够模拟病毒变种的制作过程，不断生成新的病毒变种文件，同时检测模块也会不断检测并将结果反馈。通过两个模块的循环促进，持续快速提升 SAVE 的检测能力。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839、62300128

传真：010-62304980

网址：www.caict.ac.cn